



Agenzia per la  
Cybersicurezza Nazionale



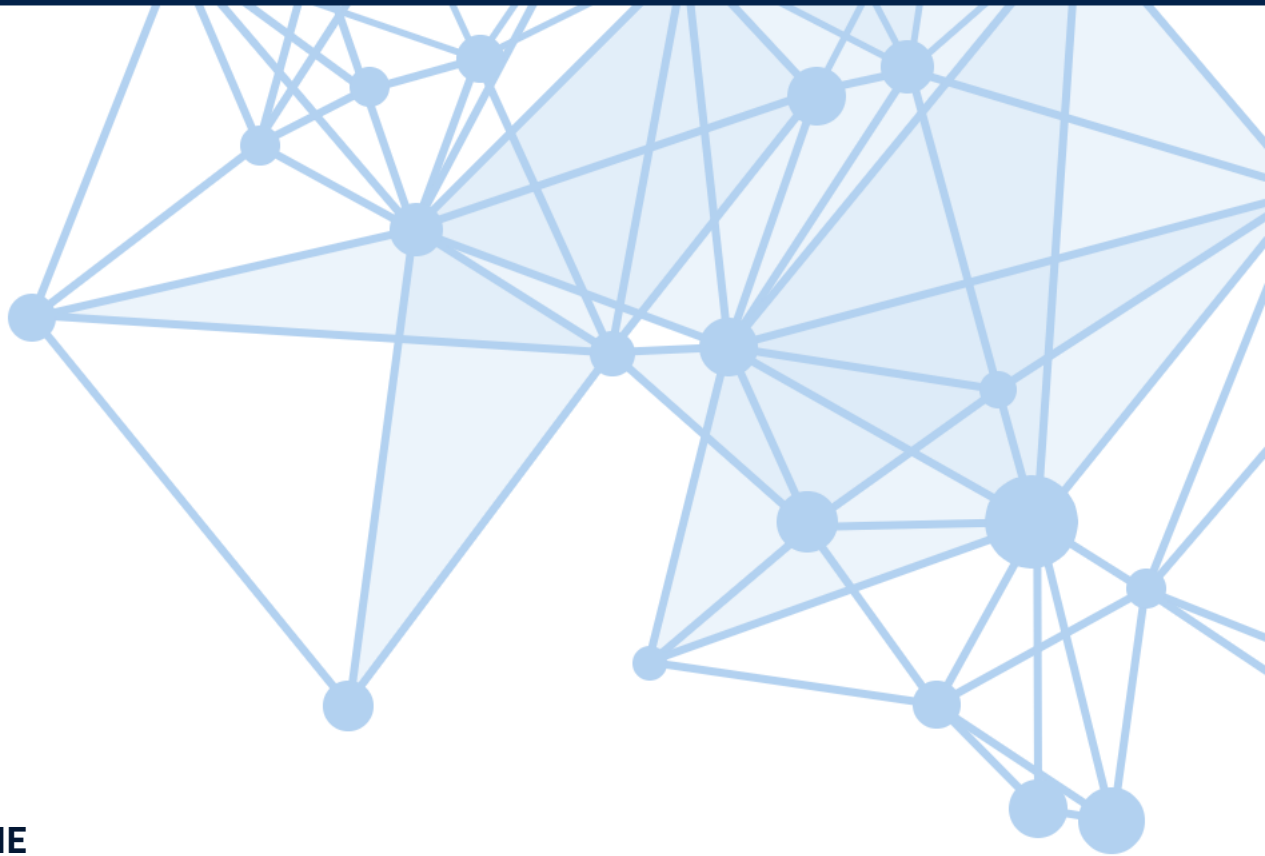
# OPERATIONAL SUMMARY

## II SEMESTRE 2025

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni  
e gestione delle crisi cyber

**TLP: CLEAR**



## INTRODUZIONE

Il presente documento presenta numeri e indicatori relativi alle attività operative svolte dall'Agenzia per la Cybersicurezza Nazionale (ACN) **nel secondo semestre del 2025, mettendoli a confronto con quelli del secondo semestre del 2024**. I dati analizzati provengono dal CSIRT Italia, articolazione tecnico-operativa dell'Agenzia e punto di riferimento nazionale per le notifiche obbligatorie e volontarie di incidenti previste dalla normativa (tra cui, Perimetro di Sicurezza Nazionale Cibernetica, Legge n. 90 del 2024, D.lgs n.138 del 2024, che recepisce la c.d. Direttiva NIS2). Il CSIRT Italia riceve inoltre informazioni da fonti aperte e commerciali, nonché da enti omologhi nazionali e internazionali, che le condividono spontaneamente o nell'ambito di accordi di collaborazione. Queste informazioni dotano l'ACN di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi o incidenti cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

- **approfondire le informazioni** a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico, quale lo studio dei malware, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- **se necessario inviare richieste di informazioni** ai soggetti;
- **fornire supporto da remoto o in loco** ai soggetti impattati;
- **inviare comunicazioni** ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati;
- **pubblicare alert o bollettini**.

Per le definizioni si rimanda al [Glossario del CSIRT Italia](#) e alla [Tassonomia Cyber dell'ACN](#) mentre per maggiori dettagli sui singoli mesi si può far riferimento agli [Operational Summary mensili](#), disponibili [pagina dedicata](#) del sito web ACN.



Le informazioni contenute in questo documento sono il risultato dell'analisi dei dati disponibili al momento della redazione; esse potrebbero essere aggiornate a seguito di nuove evidenze o di ulteriori approfondimenti.

Documento rilasciato con licenza **Creative Commons Attribuzione 4.0 Internazionale (CC BY 4.0)**.  
Testo completo della licenza disponibile su: <https://creativecommons.org/licenses/by/4.0/deed.it>



## Indice

<b>1. EXECUTIVE SUMMARY</b>	<b>5</b>
<b>2. EVENTI ED INCIDENTI</b>	<b>13</b>
<b>2.1. Settori impattati</b>	<b>14</b>
<b>2.2. Tipologia di minacce negli eventi</b>	<b>15</b>
<b>2.3. Distribuzione delle minacce per settore</b>	<b>16</b>
<b>2.4. Distribuzione geografica delle vittime</b>	<b>17</b>
<b>3. VULNERABILITÀ</b>	<b>18</b>
<b>3.1. Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia</b>	<b>18</b>
<b>3.2. Distribuzione delle vulnerabilità sui vendor</b>	<b>21</b>
<b>3.3. CWE nel II semestre 2025</b>	<b>23</b>
<b>4. MINACCIA</b>	<b>24</b>
<b>4.1. Ransomware: distribuzione delle vittime</b>	<b>24</b>
<b>4.2. Rivendicazioni ransomware</b>	<b>25</b>
<b>4.3. Rivendicazioni DDoS</b>	<b>26</b>
<b>5. MONITORAGGIO</b>	<b>27</b>
<b>5.1. Comunicazioni dirette</b>	<b>29</b>

## Elenco delle figure

Figura 1 - indicatori delle attività operative nel II semestre 2025 e nel II semestre 2024	8
Figura 2 - andamento del numero di eventi e incidenti del II semestre 2025	13
Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto al II semestre 2024 (top 15)	14
Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al II semestre 2024	15
Figura 5 - numero di vittime per settore e tipologia di minacce	16
Figura 6 - distribuzione delle vittime degli eventi cyber	17
Figura 7 - top 20 produttori affetti da vulnerabilità nel II semestre 2025 e II semestre 2024	21
Figura 8 - top 20 prodotti affetti da vulnerabilità nel II semestre 2025 e II semestre 2024	22
Figura 9 - top 5 CWE nel II semestre 2025	23
Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità	24
Figura 11 - andamento delle rivendicazioni Ransomware	25
Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni	25
Figura 13 - andamento delle rivendicazioni DDoS	26
Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni	26
Figura 15 - Numero di asset a rischio segnalati suddivisi per categoria	28
Figura 16 - Tipologia e gravità delle vulnerabilità rinvenute e segnalate negli asset a rischio	28
Figura 17 - distribuzione delle segnalazioni per tipologia di soggetto	29

## 1

# EXECUTIVE SUMMARY

## ▪ Eventi e Incidenti

Nel secondo semestre 2025 ACN ha censito **1.253 eventi cyber**, in **aumento** del **30%** rispetto allo stesso periodo dell'anno precedente (II semestre 2024). Il numero di **incidenti con impatto confermato** è stato pari a **304**, in **diminuzione** del **-25%**. L'aumento del numero complessivo di eventi è riconducibile, da un lato, al rafforzamento delle capacità di rilevazione e classificazione del CSIRT Italia, che ha consentito una più efficace individuazione di minacce, fattori di rischio e compromissioni, nonché al mutato quadro normativo, in particolare a seguito dell'entrata in vigore della Legge n. 90/2024 e del D.lgs. n. 138 del 2024; dall'altro lato, l'incremento osservato risulta associato prevalentemente alla maggiore incidenza di campagne **DDoS**, a eventi di **esposizione di dati** e a attività di **phishing**, ed altre minacce che spesso non si sono tradotte in incidenti.

## ▪ Settori interessati

Il maggior numero di vittime di eventi sono state registrate nei settori della **Pubblica amministrazione locale**, **Pubblica amministrazione centrale** e **Telecomunicazioni**. Per quanto riguarda la Pubblica Amministrazione, sia centrale sia locale,

l'elevato numero di eventi rilevati risulta determinato principalmente dalle campagne **DDoS**, quasi sempre senza impatto, e dalle **esposizioni di dati**: dati afferenti a soggetti pubblici rinvenuti dal monitoraggio su forum di scambio/vendita, su data leak sites, o altre piattaforme. Nel caso della Pubblica Amministrazione locale, si osservano diversi casi in cui la compromissione o l'indisponibilità di fornitori di servizi web, hanno generato ripercussioni a catena su più amministrazioni, contribuendo ad amplificare il numero complessivo di soggetti coinvolti. Nel settore delle Telecomunicazioni, si è osservata una crescente incidenza di compromissioni di caselle di posta elettronica associate ad utenze private.

## ▪ Ransomware

Il ransomware rappresenta una delle tipologie di minaccia più impattanti sull'operatività delle vittime. Nel II semestre 2025, gli incidenti riconducibili ai ransomware si sono mantenuti complessivamente stabili rispetto al periodo precedente, attestandosi a **54 casi**, a fronte dei **48** registrati nel II semestre 2024. I settori maggiormente interessati risultano essere **Manifatturiero**, **Vendita al dettaglio** e **Tecnologico**. Gli attacchi ransomware hanno interessato in larga

misura piccole imprese, caratterizzate da capacità di cybersicurezza limitate. I principali fattori abilitanti per le campagne ransomware osservate sono: l'utilizzo di credenziali valide, precedentemente compromesse; lo sfruttamento di vulnerabilità non sanate e l'utilizzo di servizi di accesso remoto (come le VPN) non correttamente configurati o protetti.

#### ▪ **Attacchi DDoS**

Per quanto riguarda i **DDoS**, si è osservato un **aumento** del 101% nel II semestre 2025 con **366** attacchi rispetto ai **182** del II semestre 2024. Tali campagne DDoS, riconducibili a dinamiche **hacktiviste**, si sono sviluppate in un contesto internazionale caratterizzato da tensioni geopolitiche, manifestandosi secondo fasi di diversa frequenza e intensità, **senza tuttavia determinare effetti operativi significativi o duraturi sui sistemi e sui servizi dei soggetti nazionali coinvolti**. Gli impatti sono stati – come di consueto per questo tipo di attività – mitigati efficacemente dai soggetti italiani, anche grazie all'attività di allertamento del CSIRT Italia, che comunica tempestivamente contromisure ai soggetti interessati. In questo semestre, solo il **7%** degli attacchi ha causato impatti misurabili (ovvero disservizi transienti per gli utenti dei portali attaccati tipicamente della durata di qualche ora). Nel periodo considerato, i settori maggiormente interessati dalle campagne DDoS sono risultati la **Pubblica Amministrazione**, i **Trasporti** e le **Telecomunicazioni**. Nel complesso, i dati semestrali mostrano una progressiva attenuazione dell'attività hacktivista.

#### ▪ **Phishing**

Nel II semestre 2025 si è registrato un aumento del numero complessivo di eventi di phishing. Gli episodi di maggiore rilevanza hanno interessato prevalentemente la **Pubblica Amministrazione**, il settore **Sanitario** e quello dei **Trasporti**. Le campagne rilevate sono state principalmente orientate all'acquisizione non autorizzata di credenziali di accesso per servizi cloud, mediante l'impiego di link malevoli inviati tramite e-mail. In tale contesto, si segnala una campagna di phishing di particolare intensità che ha coinvolto una struttura ospedaliera, destinataria di oltre 3.000 messaggi e-

mail fraudolenti, finalizzati alla compromissione delle caselle di posta elettronica del personale. Il CSIRT Italia complessivamente nel II semestre 2025 ha individuato e segnalato **927 URL di phishing**, a fronte delle **579** del II semestre 2024.

#### ▪ **Esposizione dati**

Nel secondo II semestre 2025 i fenomeni di **esposizione dati** hanno rappresentato una componente ricorrente del quadro della minaccia, registrando un incremento significativo rispetto al secondo semestre 2024. Nell'ambito delle attività di monitoraggio delle principali piattaforme di scambio illecito di dati, nel II semestre 2025 sono stati rilevati complessivamente **232** eventi di esposizione, a fronte dei 153 registrati nel II semestre 2024. Nel periodo considerato, hanno suscitato particolare attenzione, nel mese di agosto, le esposizioni documenti di identità digitali, verosimilmente conseguenti alla compromissione di credenziali associate a soluzioni software per il check-in alberghiero. Nel mese di settembre, sono stati osservati eventi di esposizione dati a danno di fornitori di **Servizi digitali**, **Servizi finanziari** e **Università**. Nel mese di novembre, l'attività si è concentrata prevalentemente sul fenomeno delle credenziali compromesse, con il riscontro di **112 account istituzionali** esposti a seguito di compromissione da **infostealer**. Nel mese di dicembre, i fenomeni di esposizione di dati hanno rappresentato la tipologia di minaccia maggiormente rilevata. In relazione a tali eventi, il CSIRT Italia ha provveduto a effettuare tempestive attività di comunicazione nei confronti dei soggetti istituzionali interessati.

#### ▪ **Monitoraggio proattivo**

Nell'ambito dell'attività proattiva di monitoraggio della superficie esposta dei soggetti nazionali, il CSIRT Italia ha inviato complessivamente **5.205** comunicazioni di allertamento a pubbliche amministrazioni e imprese appartenenti alla constituency, relative all'esposizione su Internet di **15.360** servizi a rischio, riconducibili all'impiego di prodotti e componenti potenzialmente vulnerabili. In particolare, sono state riscontrate evidenze di sfruttamento attivo di vulnerabilità in

**Microsoft SharePoint** on-premises, nonché esposizioni su internet di piattaforme **Citrix NetScaler** e soluzioni **Fortinet FortiWEB**. Nel medesimo periodo, sono stati inoltre identificati e allertati a livello nazionale i soggetti con dispositivi di rete esposti e potenzialmente compromessi dalla botnet **Raptor Train**, attribuita in alcuni report al gruppo Flax Typhoon, in relazione a un'operazione coordinata dall'FBI e dal Dipartimento di Giustizia americano.

A seguito della pubblicazione di un **Cybersecurity Advisory** congiunto (NSA, CISA, FBI, DC3; per l'Italia AISE/AISI), il CSIRT Italia ha condotto specifiche attività di analisi, identificando 36 soggetti a rischio sulla base di indicatori di compromissione (IOC) e di tattiche, tecniche e procedure (TTP). Le attività di monitoraggio hanno inoltre consentito di individuare esposizioni di telecamere IP sfruttate da gruppi hacktivisti e di ricostruire un'infrastruttura nazionale di distribuzione di malware, associata alle famiglie **Purple Fox**, **Amadey**, **Agent Tesla** e **GootLoader**, per la quale sono state avviate azioni di allertamento e mitigazione.

Nel corso del semestre sono state altresì rilevate vulnerabilità su apparati **F5**, con potenziali impatti in termini di *Denial of Service*, *Remote Code Execution* e *Privilege Escalation*. Ulteriori attività di allertamento hanno riguardato le vulnerabilità **WatchGuard Firebox** (CVE-2025-59396) e **SolarWinds Web Help Desk** (CVE-2025-40549 / CVE-2025-40548 / CVE-2025-40547), nonché nuove evidenze di utilizzo della webshell **BadCandy**, con potenziale impatto su **Cisco IOS XE**.

Tra le principali attività del periodo ha infine assunto

particolare rilievo la gestione della vulnerabilità critica CVE-2025-55182, relativa a **Meta React Server**, che ha richiesto specifiche attività di allertamento nei confronti dei soggetti potenzialmente interessati.

#### ▪ **Vettori di attacco**

I punti d'ingresso più frequenti delle attività malevole censite sono stati: **campagne malevole via e-mail**, **sfruttamento di vulnerabilità** e l'impiego di **credenziali valide** precedentemente compromesse, in linea con quanto registrato nel 2024.

#### ▪ **Vulnerabilità**

Il numero di **nuove vulnerabilità (CVE)** pubblicate nell'ambito del CVE program ([www.cve.org](http://www.cve.org)) è stato pari a **25.319**, sostanzialmente allineato rispetto al II semestre 2024.

#### ▪ **Allertamento**

Nel II semestre 2025 il CSIRT Italia ha inviato **23.724 comunicazioni dirette** ai fini di allertamento preventivo, a seguito dell'individuazione di asset compromessi, vulnerabili o esposti in maniera inopportuna, o per altri fattori di rischio, nei confronti dei soggetti della constituency nazionale. Nel II semestre 2024 le comunicazioni inviate a tal scopo furono **32.246**. Oltre alle comunicazioni dirette, nel II semestre 2025 sono stati pubblicati **407 alert** sul sito web del CSIRT Italia (<https://www.acn.gov.it/portale/csirt-italia>), relativi a vulnerabilità e fattori di rischio, corredati dalle necessarie contromisure, mentre, nel corso del II semestre 2024 gli alert pubblicati sono stati **298**.

Il prosieguo del documento presenta, in **questo Capitolo**, i principali numeri e le vulnerabilità del II semestre 2025; nel **Capitolo 2** un focus sugli eventi e incidenti, con settori impattati, tipologia di minacce rilevate e loro distribuzione sui settori nonché distribuzione geografica delle vittime; nel **Capitolo 3** un approfondimento sulle **vulnerabilità** più gravi del semestre con la loro distribuzione sui vendor e le CWE più comuni; i dettagli sulle **minacce ransomware, DDoS e malware** sono riportati nel **Capitolo 4** mentre il **Capitolo 5** mostra i risultati del **monitoraggio proattivo**, con i numeri e le tipologie di dispositivi e servizi a rischio individuati dal CSIRT Italia.

Per maggiori dettagli sui singoli mesi del II semestre 2025 si può far riferimento agli *Operational Summary* mensili, disponibili pagina dedicata del sito web ACN.

# I NUMERI DEL II SEMESTRE 2025

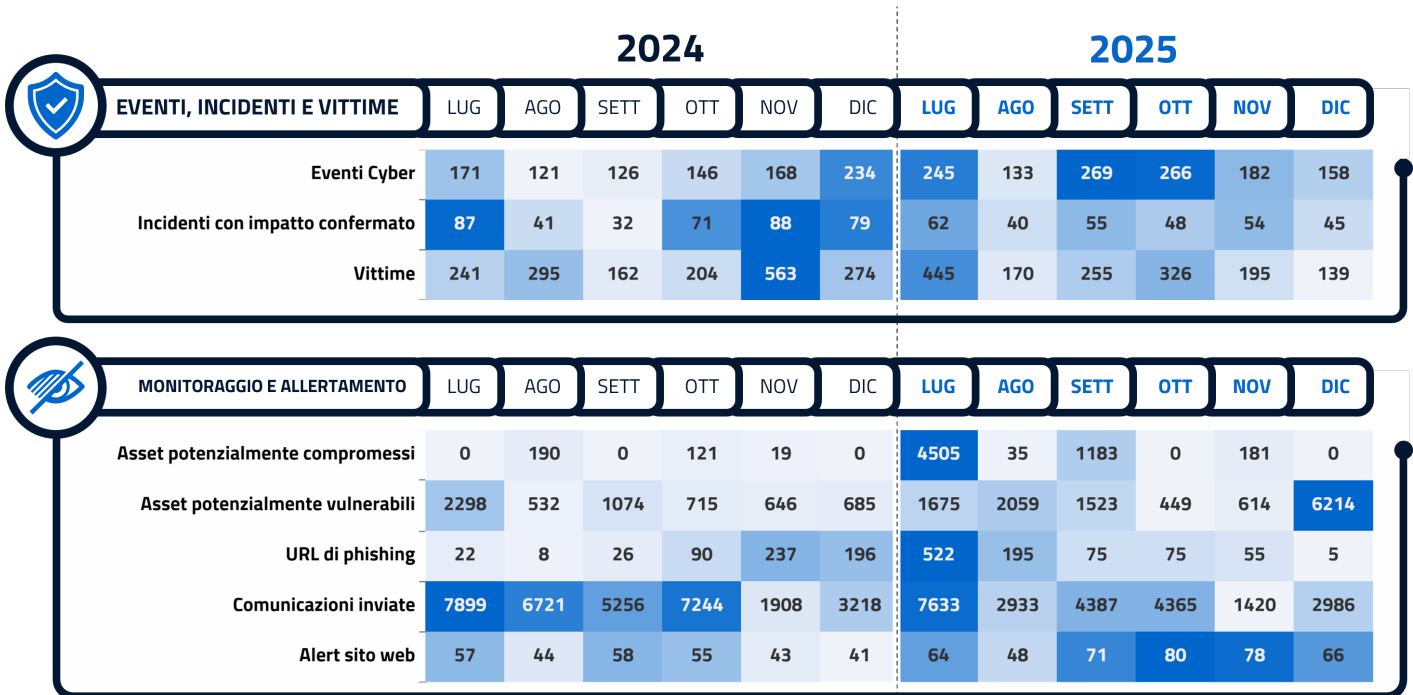


Figura 1 - indicatori delle attività operative nel II semestre 2025 e nel II semestre 2024

- **1.253** eventi cyber, in **aumento (+287)**;
- **1.535** vittime, in **diminuzione (-202)**;
- **447** vittime della constituency<sup>1</sup>, in **diminuzione (-110)**;
- **304** incidenti con impatto confermato, in **diminuzione (-94)**;
- **5.904** asset potenzialmente compromessi, in **aumento (+5.574)**;
- **12.534** asset potenzialmente vulnerabili, in **aumento (+6.584)**;
- **407** alert sul sito web del CSIRT Italia, in **aumento (+109)**;
- **23.724** comunicazioni inviate, in **diminuzione (-8.522)**;
- **25.319** nuove CVE, in **aumento (+5.762)**.

<sup>1</sup>La constituency è l'insieme dei soggetti che operano nei settori NIS, Perimetro, Telco o nella Pubblica amministrazione, nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi cibernetici. Sul sito ACN è disponibile un documento di approfondimento sulla constituency del CSIRT Italia.

# PRODOTTI VULNERABILI

Di seguito una selezione delle vulnerabilità particolarmente importanti, organizzate per prodotto o produttore che nel II semestre 2025 sono stati oggetto di specifici alert pubblicati sul sito web del CSIRT Italia o di allertamento tramite comunicazioni dirette. **I soggetti utilizzatori di tali prodotti sono invitati a verificare l'avvenuta adozione delle azioni di mitigazioni rilasciate dal vendor o riportate negli alert referenziati di seguito.**

## Luglio:

- **Citrix NetScaler ADC e Gateway** (CVE-2025-5777) Link all>alert;
- **Microsoft SharePoint** (CVE-2025-53770, CVE-2025-53771) Link all>alert;
- **Fortinet FortiWeb e FortiVoice** (CVE-2025-25257, CVE-2025-47856) Link all>alert;
- **Sudo project** (CVE-2025-32462, CVE-2025-32463) Link all>alert;
- **PHP** (CVE-2025-1220, CVE-2025-1735, CVE-2025-6491) Link all>alert;
- **Prodotti VMware (Cloud Foundation ESX, vSphere Foundation ESX, ESXi, Workstation, Fusion, Cloud Foundation, Telco Cloud Platform, Telco Cloud Infrastructure e VMware Tools)** (CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239) Link all>alert;
- **Node.js** (CVE-2025-27209, CVE-2025-27210) Link all>alert;
- **Wing FTP Server** (CVE-2025-47812) Link all>alert;
- **Ivanti Endpoint Manager Mobile (EPMM)** (CVE-2025-6771, CVE-2025-6770) Link all>alert;
- **AMI MegaRAC** (CVE-2024-54085) Link all>alert;
- **CrushFTP** (CVE-2025-54309) Link all>alert;
- **XWiki** (CVE-2025-32429) Link all>alert;
- **Cisco ISE (Identity Services Engine) ed ISE-PIC (Passive Identity Connector)** (CVE-2025-20281, CVE-2025-20282, CVE-2025-20337) Link all>alert;
- **Cisco Unified Communications Manager** (CVE-2025-20309) Link all>alert;
- **PaperCut NG/MF** (CVE-2023-2533) Link all>alert;
- **WildFly Jboss** (CVE-2017-12149, CVE-2015-7501, CVE-2011-4085, CVE-2010-0738) Link all>alert.

## Agosto:

- **SonicWall Firewall** (CVE-2025-40766) Link all>alert;
- **Sangoma FreePBX** (CVE-2025-57819) Link all>alert;
- **Adobe Experience Manager** (CVE-2025-54254, CVE-2025-54253) Link all>alert;
- **Citrix NetScaler e Gateway** (CVE-2025-8424, CVE-2025-7776, CVE-2025-7775) Link all>alert;
- **Fortinet FortiSIEM, FortiWeb, FortiOS, FortiPAM, FortiProxy, FortiSwitchManager** (CVE-2024-26009, CVE-2025-52970, CVE-2025-25256) Link all>alert;
- **Directus** (CVE-2025-55746) Link all>alert;
- **Cisco IOS-XE** (CVE-2023-20273) Link all>alert;
- **Palo Alto Networks PAN-OS** (CVE-2024-3400) Link all>alert;
- **Salesforce Tableau Server** (CVE-2025-26496) Link all>alert;
- **Plex Media Server** (CVE-2025-34158) Link all>alert;
- **Commvault CommCell** (CVE-2025-57789, CVE-2025-57790, CVE-2025-57791, CVE-2025-57788) Link all>alert;
- **N-able N-central** (CVE-2025-8876, CVE-2025-8875)

- Link all>alert;
- **Microsoft Exchange** (CVE-2025-53786) Link all>alert;
  - **Samsung magicINFO 9** (CVE-2025-54451) Link all>alert;
  - **Citrix NetScaler e Gateway** (CVE-2025-5777) Link all>alert;
  - **SonicWall SMA100 series** (CVE-2025-40598, CVE-2025-40597, CVE-2025-40596) Link all>alert;
  - **Microsoft SharePoint** (CVE-2025-53771, CVE-2025-53770) Link all>alert;
  - **Squid** (CVE-2025-54574) Link all>alert;
  - **Mitel MiCollab** (CVE-2025-52914) Link all>alert.
- 

## Settembre:

- **Cisco Adaptive Security Appliance, Cisco Firewall Threat Defense, Cisco IOS, Cisco IOS XE e Cisco IOS XR** (CVE-2025-20363, CVE-2025-20362, CVE-2025-20333) Link all>alert;
  - **Formbricks** (CVE-2025-59934) Link all>alert;
  - **Notepad++** (CVE-2025-56383) Link all>alert;
  - **VMware Tools for Windows, Aria Operations, VCF operations, NSX, vCenter** (CVE-2025-41246, CVE-2025-41245, CVE-2025-41244, CVE-2025-41252, CVE-2025-41251, CVE-2025-41250) Link all>alert;
  - **TP-Link Archer C7(EU) V2, TL-WR841N/ND(MS) V9 TL-WR841N** (CVE-2025-9377, CVE-2023-50224) Link all>alert;
  - **Ivanti Connect Secure** (CVE-2025-55144, CVE-2025-55143, CVE-2025-55142, CVE-2025-55141, CVE-2025-55139, CVE-2025-55148, CVE-2025-55147, CVE-2025-55146, CVE-2025-55145, CVE-2025-8711 e CVE-2025-8712) Link all>alert;
  - **Django** (CVE-2023-57833) Link all>alert;
  - **Sangoma FreePBX** (CVE-2025-57819) Link all>alert;
  - **GitLab** (CVE-2025-6454) Link all>alert;
  - **SAP Netweaver** (CVE-2025-42958, CVE-2025-42922 e CVE-2025-42944) Link all>alert;
  - **Digiever NVR** (CVE-2025-10265, CVE-2025-10264) Link all>alert;
  - **WatchGuard Fireware** (CVE-2025-9242) Link all>alert;
  - **GoAnywhere MFT** (CVE-2025-10035) Link all>alert;
  - **FlowiseAI** (CVE-2025-58434) Link all>alert;
  - **Omnissa Workspace ONE UEM** (CVE-2025-25231) Link all>alert;
  - **Argo-CD** (CVE-2025-55190) Link all>alert;
  - **SolarWinds Web Help Desk** (CVE-2025-26399) Link all>alert;
  - **Progress OpenEdge** (CVE-2025-7388) Link all>alert;
  - **Ivanti Endpoint Manager Mobile** (CVE-2025-4428 e CVE-2025-4427) Link all>alert;
- 

## Ottobre:

- **Microsoft Windows Server 2019** (CVE-2025-59287) Link all>alert;
- **ISC BIND 9** (CVE-2025-8677, CVE-2025-40780, CVE-2025-40778) Link all>alert;
- **Gladinet CentreStack and TrioFox** (CVE-2025-11371) Link all>alert;
- **WatchGuard Fireware OS** (CVE-2025-9242) Link all>alert;
- **Oracle Concurrent Processing** (CVE-2025-61882) Link all>alert;
- **F5 F5OS e BIG-IP** (CVE-2025-53521, CVE-2025-53474, CVE-2025-48008, CVE-2025-46706 e CVE-2025-41430) Link all>alert;
- **Apache Tomcat** (CVE-2025-55752 e CVE-2025-55574) Link all>alert;
- **Zimbra Collaboration Suite** (CVE-2025-62763) Link all>alert;
- **ISC BIND** (CVE-2025-40778) Link all>alert;

- **Libraesva Email Security Gateway** (CVE-2025-59689) Link all>alert;
- **Squid** (CVE-2025-62168) Link all>alert;
- **SAP Netweaver** (CVE-2025-42944) Link all>alert;
- **TP-Link Gateway Omada** (CVE-2025-7851, CVE-2025-7850, CVE-2025-6542 e CVE-2025-6541) Link all>alert;
- **Telerik UI** (CVE-2025-3600) Link all>alert;
- **Nagios Log Server** (CVE-2025-44824 e CVE-2025-44823) Link all>alert;
- **Microsoft ASP.NET Core 8.0** (CVE-2025-55315) Link all>alert;
- **Ivanti Connect Secure** (CVE-2025-22457) Link all>alert;
- **Microsoft Windows Server Update Service** (CVE-2025-59287) Link all>alert;
- **Atlassian Jira** (CVE-2025-22167) Link all>alert;
- **Mattermost** (CVE-2025-58075 e CVE-2025-58073) Link all>alert;
- **Veeam Backup & Replication** (CVE-2025-48984 e CVE-2025-48983) Link all>alert;
- **DNN** (CVE-2025-64095) Link all>alert;
- **Redis** (CVE-2025-49844) Link all>alert;
- **Adobe Commerce/Magento** (CVE-2025-54236) Link all>alert;
- **Netbird** (CVE-2025-10678) Link all>alert;
- **FlowiseAI** (CVE-2025-61913) Link all>alert;
- **Gladinet CentreStack e TrioFox** (CVE-2025-11371) Link all>alert;
- **Fortinet FortiSwitchManager** (CVE-2025-49201) Link all>alert;
- **Oracle E-Business Suite** (CVE-2025-61884, CVE-2025-62481 e CVE-2025-53072) Link all>alert; Link all>alert;
- **VMware Aria Operations** (CVE-2025-41244) Link all>alert;
- **Ivanti Endpoint Manager** (CVE-2025-9713 e CVE-2025-11622) Link all>alert;

## Novembre:

- **Grafana Labs** (CVE-2025-41115) Link all>alert;
- **React Native Community** (CVE-2025-11953) Link all>alert;
- **Gladinet Triofox** (CVE-2025-12480) Link all>alert;
- **D-Link DIR-878** (CVE-2025-60676, CVE-2025-60674, CVE-2025-60673, CVE-2025-60672) Link all>alert;
- **SolarWinds Web Help Desk** (CVE-2025-40549, CVE-2025-40548 e CVE-2025-40547) Link all>alert;
- **Django** (CVE-2025-64459) Link all>alert;
- **Open Source Geospatial Foundation GeoServer** (CVE-2025-58360) Link all>alert;
- **Fortinet FortiWeb** (CVE-2025-58034) Link all>alert;
- **PostgreSQL pgAdmin** (CVE-2025-12762) Link all>alert;
- **W3 Total Cache** (CVE-2025-9501) Link all>alert;
- **Open WebUI** (CVE-2025-64495) Link all>alert;
- **Symfony** (CVE-2025-64500) Link all>alert;
- **OpenWRT** (CVE-2025-62526 e CVE-2025-62525) Link all>alert;
- **Monsta FTP** (CVE-2025-34299) Link all>alert;
- **Twonky Server** (CVE-2025-13316 e CVE-2025-13315) Link all>alert;
- **Asus AiCloud** (CVE-2025-59366) Link all>alert;
- **R.V.R Elettronica TEX** (CVE-2025-63207) Link all>alert;
- **Apache OFBiz** (CVE-2025-61623 e CVE-2025-59118) Link all>alert;
- **N-Able N-Central** (CVE-2025-11700) Link all>alert;

## Dicembre:

- **Meta React DIR-878** (CVE-2025-55182, CVE-2025-67779, CVE-2025-55184) Link all>alert;
- **Google Chrome** (CVE-2025-14174) Link all>alert;
- **Cisco** (CVE-2025-20393) Link all>alert;
- **MongoDB Triofox** (CVE-2025-14847) Link all>alert;
- **Gogs** (CVE-2025-8110) Link all>alert
- **WatchGuard Fireware OS** (CVE-2025-14733) Link all>alert
- **Moodle** (CVE-2025-67855, CVE-2025-67850, CVE-2025-67848, CVE-2025-67847, CVE-2025-67849) Link all>alert
- **Fortinet FortiSwitchManager, FortiProxy, FortiOS e FortiWeb** (CVE-2025-59718, CVE-2025-59719) Link all>alert
- **SonicWall SMA1000** (CVE-2025-40602) Link all>alert
- **Mattermost** (CVE-2025-12419, CVE-2025-12421) Link all>alert
- **Microsoft ASP.NET Core 8.0, ASP.NET Core 9.0, ASP.NET Core 2.3, Microsoft Visual Studio 2022 version 17.12, Microsoft Visual Studio 2022 version 17.10 e Microsoft Visual Studio 2022 version 17.14** (CVE-2025-55315) Link all>alert
- **NopSolutions nopCommerce** (CVE-2025-11699)
- **Traccar** (CVE-2025-61666)
- **N8n-io n8n** (CVE-2025-68613) Link all>alert
- **Gladinet CentreStack and TrioFox** (CVE-2025-14611) Link all>alert
- **Vega** (CVE-2025-59840) Link all>alert
- **Xwiki xwiki-platform** (CVE-2025-55749) Link all>alert
- **ConnectWise ScreenConnect** (CVE-2025-14265)
- **Cisco Secure Email e Secure Email and Web Manager** (CVE-2025-20393) Link all>alert

# 2

## EVENTI ED INCIDENTI

Nel II semestre 2025 sono stati individuati **1.253** eventi cyber, in **aumento** del 30% rispetto al II semestre 2024. Questi ultimi hanno **interessato 830 soggetti nazionali**<sup>2</sup>: 447 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 1.253 eventi cyber, **304 sono stati classificati quali incidenti**, in **diminuzione** del 25% rispetto a quelli registrati nel II semestre 2024. I valori massimi registrati nei mesi di luglio, settembre e ottobre risultano prevalentemente associati alle campagne DDoS condotte da gruppi hacktivisti. La Figura 2 mostra l'andamento del numero di eventi e incidenti del semestre, evidenziandone la media del periodo.

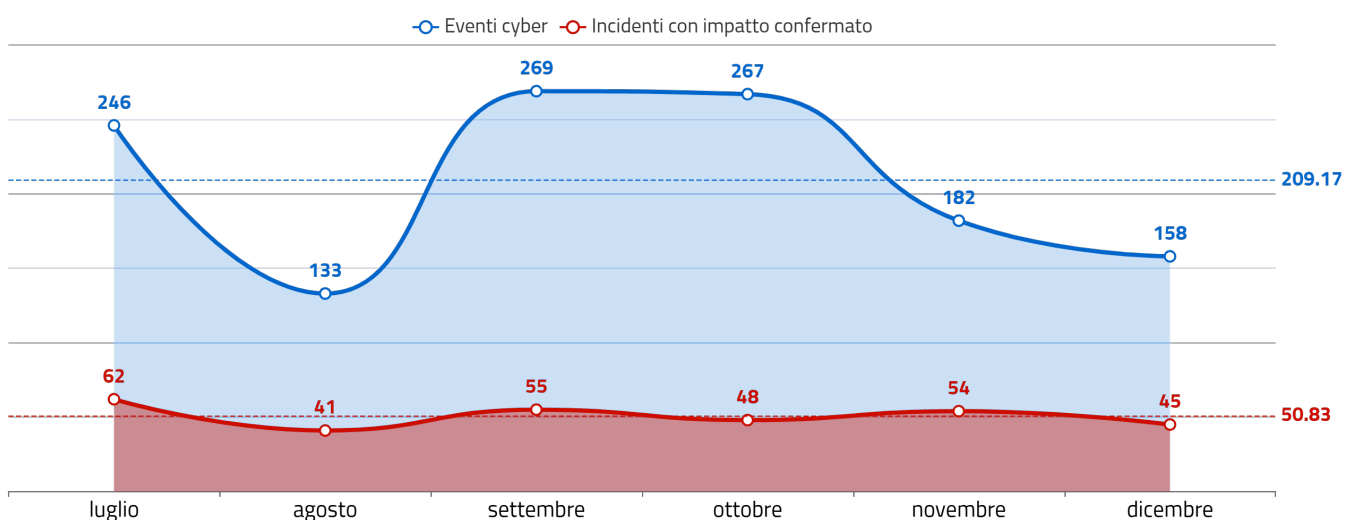


Figura 2 - andamento del numero di eventi e incidenti del II semestre 2025

<sup>2</sup>Alcuni soggetti sono stati interessati più volte. Il numero di vittime non univoche è stato 1.535.

## 2.1 Settori impattati

In Figura 3 si riporta il numero di vittime di eventi per settore impattato<sup>3</sup> nel II semestre 2025 e nel II semestre 2024. Si evidenzia altresì la variazione percentuale tra i due valori. In particolare, la Pubblica Amministrazione locale emerge come il settore più esposto nel semestre, anche in relazione ad un data breach rilevato nel mese di luglio e all'incidenza delle campagne DDoS, che hanno contribuito in modo significativo al numero complessivo di eventi rilevati.

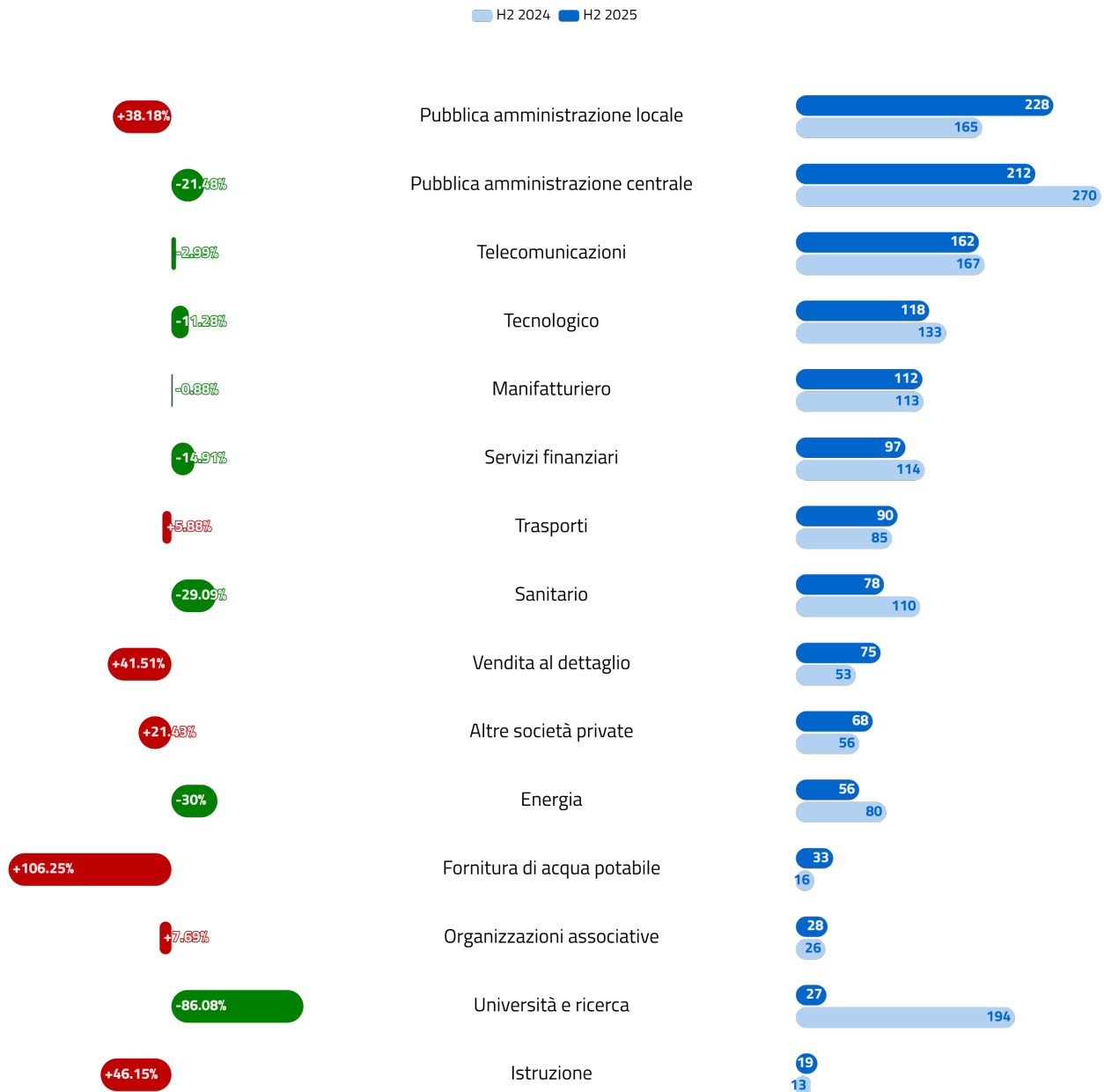


Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto al II semestre 2024 (top 15)

<sup>3</sup> Si noti che ogni evento può avere più vittime afferenti ad uno o più settori di attività e che una vittima può operare in più settori. Talvolta non è possibile associare un evento ad una vittima e la vittima ad un settore.

## 2.2 Tipologia di minacce negli eventi

In Figura 4 si riporta il numero di minacce rilevate negli eventi<sup>4</sup> nel II semestre 2025 e nel II semestre 2024. Si evidenzia altresì la variazione percentuale tra i due valori.

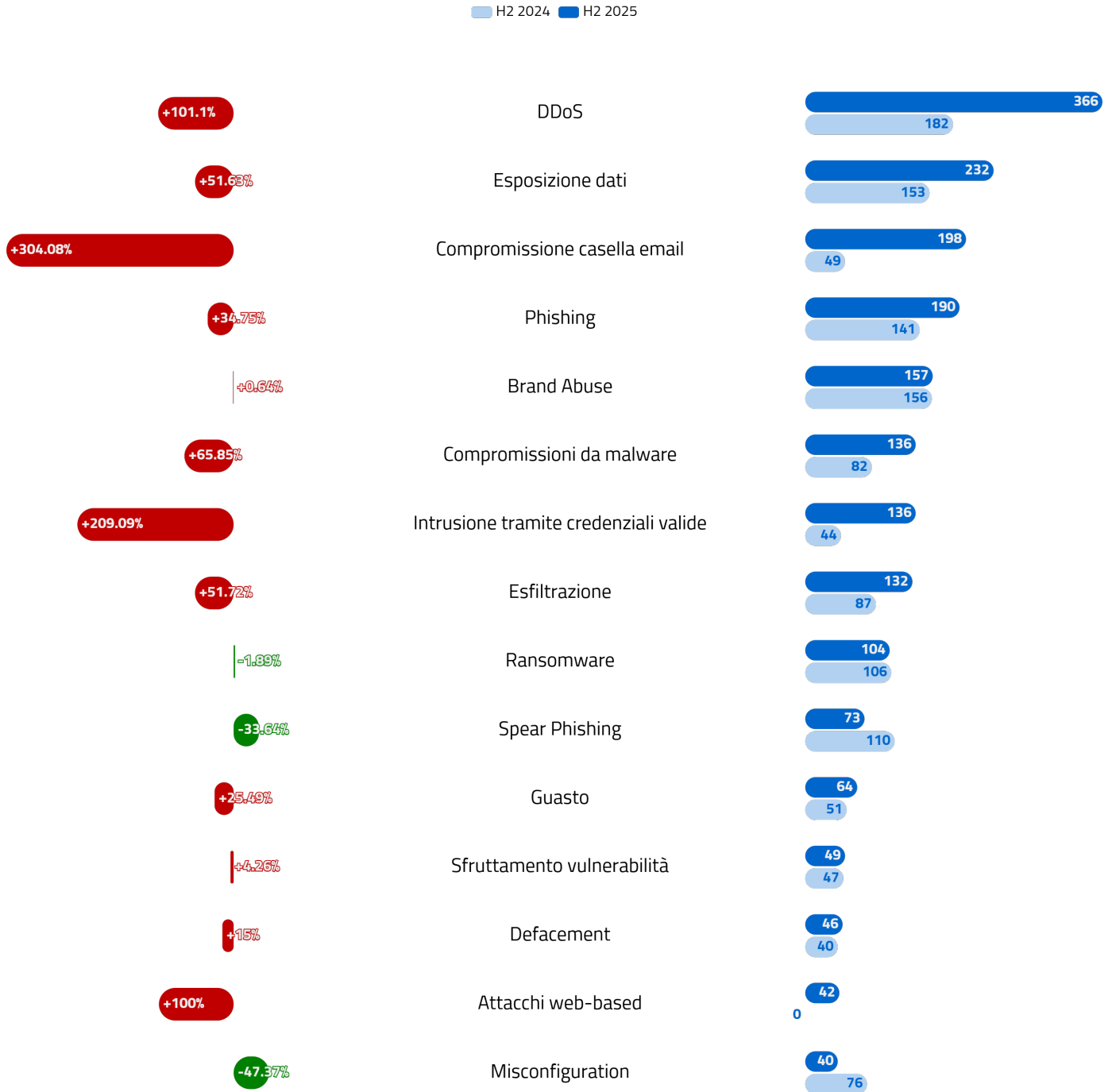


Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al II semestre 2024

<sup>4</sup> Si noti che ognuno degli eventi può essere stato associato ad una o più tipologie di minacce.

## 2.3 Distribuzione delle minacce per settore

In Figura 5 si riporta, per ogni settore, il numero di vittime che hanno subito la minaccia specificata, analizzando gli eventi del II semestre 2025. Si ricorda che ad un evento possono essere associate più minacce e più vittime. Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (<https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn>). L'analisi della distribuzione settoriale delle principali tipologie di minaccia evidenzia dinamiche differenziate. I fenomeni di esposizione di dati si configurano come trasversali, interessando soggetti appartenenti a una pluralità di settori. Le campagne DDoS hanno invece interessato prevalentemente la Pubblica Amministrazione, mentre le attività di scansione attiva su credenziali risultano anch'esse distribuite su più comparti, con una maggiore incidenza sulla Pubblica Amministrazione. In Figura sono mostrati solo i 15 settori più interessati dalle minacce.

	Settore 1	Settore 2	Settore 3	Settore 4	Settore 5	Settore 6	Settore 7	Settore 8	Settore 9	Settore 10	Settore 11	Settore 12	Settore 13	Settore 14	Settore 15
	Settore 1	Settore 2	Settore 3	Settore 4	Settore 5	Settore 6	Settore 7	Settore 8	Settore 9	Settore 10	Settore 11	Settore 12	Settore 13	Settore 14	Settore 15
Esposizione dati	30	61	34	39	41	30	30	21	18	50	18	6	2	7	12
DDoS	153	69		31	12	2	13	1	40		5	3	7		17
Compromissione casella email	17	14	18	69	11	8	4	7	9	12	9	6	4	4	
Phishing	18	36	15	4	15	12	23	8	10	11	8	6	9	1	1
Esfiltrazione	6	18	33	11	23	23	20	15	7	1	10	3		1	1
Brand Abuse	9	27	19	3	17	9	28	8	12	6	8	4	7	3	
Compromissioni da malware	14	13	20	9	16	13	4	19	2	4	9	4	2	3	1
Ransomware	3		35	2	19	23	5	17	2	3	5	1	2	4	
Intrusione tramite credenziali valide	15	11	10	27	9	10	3	6	6	10	4	4	1	3	1
Spear Phishing	9	11	13	7	5	4	3	4	4	5	7	3	2	2	
Sfruttamento vulnerabilità	7	8	9	1	10	10	1	8	1	4	4	5	4	3	
Guasto	6	6	1	25	11	1	8		6	5	2			1	1
Attacchi web-based	6	2	8	2	8	10		9	2	3	5	1	4	3	
Misconfiguration	7	12	4	7	6	6		3	3	2		2	1		
Defacement	5		5		5	8		7	1	1	2	1	3	3	
Cybersquatting		5	3		2	1	14	1	3	1			3		
Smishing		3	9	1	1		6			1	1			1	
SCADA/ICS attack			6	2	1	1		2	1		6				3
Scansione attiva su credenziali	3	3	1	8		1					1				
Diffusione malware tramite email	7	1	1		1	3					2	1	1		
Scansioni attive sul perimetro di rete		1	1	1	5	2	1		2	1	1	1			
Typosquatting		1	2		3		2	1	1			1			
Supply chain attack	1	2			2	1		1			1				
DoS	1	2			1							1			
Spam e scam		2	1		1										
Tentativi di frode			1												

Figura 5 - numero di vittime per settore e tipologia di minacce

## 2.4 Distribuzione geografica delle vittime

I 1.253 eventi cyber hanno interessato **1.535** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

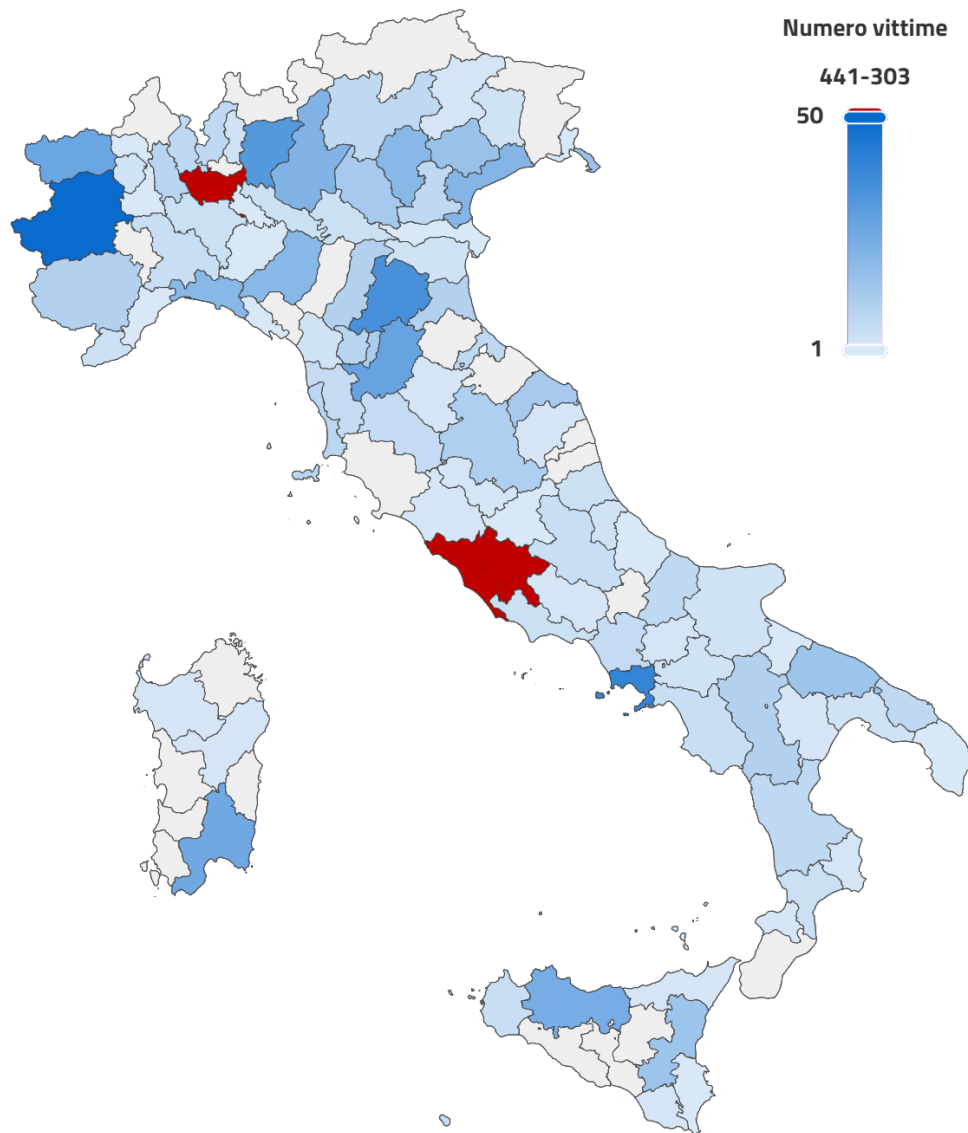


Figura 6 - distribuzione delle vittime degli eventi cyber

## 3

# VULNERABILITÀ

Nel II semestre 2025 sono state pubblicate<sup>5</sup> **25.319** nuove CVE, in **aumento (+5.762)** rispetto al II semestre 2024. Le più gravi di queste divengono oggetto di comunicazioni dirette da parte del CSIRT Italia ai soggetti della constituency e di specifico alert sul sito web, corredati dalle contromisure da adottare. In questa sezione si riportano quelle più gravi oggetto di alert, evidenziando il prodotto affetto e il link all'alert sul sito web. Le vulnerabilità vengono altresì analizzate e organizzate per vendor, per prodotto e per tipologia, come mostrato più avanti.

All'indirizzo <https://www.acn.gov.it/portale/csirt-italia/alert-e-bollettini> è possibile accedere a tutti gli altri alert pubblicati.

## 3.1 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Nel II semestre 2025 gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **407**. Le vulnerabilità particolarmente gravi, riportate di seguito ordinate per stima d'impatto sistemico<sup>6</sup>, sono state quelle relative a prodotti di:

- **SonicWall**: ricercatori di sicurezza hanno recentemente rilevato attività anomale relative a una possibile vulnerabilità di tipo zero-day nel servizio SSLVPN di alcuni modelli di firewall SonicWall Gen 7. Tale vulnerabilità consentirebbe a utenti malintenzionati di eludere i meccanismi di autenticazione anche qualora siano abilitate soluzioni multi-fattore (MFA) sui sistemi target (stima di impatto sistemico **84,35/100**). Link all'alert del 05/08/2025;
- **Ollama**: rilevata una nuova vulnerabilità in Ollama, noto progetto open source, utilizzato per eseguire LLM localmente sulla propria infrastruttura, supportando vari modelli come gpt-oss, DeepSeek-R1, Meta Llama4, Google Gemma3. Tale vulnerabilità, qualora sfruttata, permetterebbe ad un utente malintenzionato, con accesso all'API di Ollama,

<sup>5</sup>Dati del National Vulnerability Database <https://nvd.nist.gov/vuln> del NIST. Il database completo delle CVE è pubblicamente accessibile <https://cve.mitre.org/>.

<sup>6</sup>La stima d'impatto sistemico è un valore da 0 a 100, associato a ogni vulnerabilità esaminata dal CSIRT Italia tenendo conto di diversi parametri, tra i quali il CVSS, la disponibilità di patch/workaround e Proof of Concept (POC), la diffusione dei software/dispositivi interessati nella constituency.

- di caricare un model malevolo ed eseguire codice arbitrario remoto (stima di impatto sistemico **84,35/100**). Link all'alert del 05/11/2025;
- **Meta:** rilasciati aggiornamenti di sicurezza che risolvono tre vulnerabilità, di cui due con gravità "alta", in Reat Server Components. Tali vulnerabilità, qualora sfruttate, potrebbero consentire ad un utente malintenzionato di compromettere la disponibilità del servizio sui sistemi interessati (stima di impatto sistemico **79,48/100**). Link all'alert del 03/12/2025;
  - **Sangoma:** rilevato lo sfruttamento attivo di una vulnerabilità zero-day con gravità "critica" in FreePBX, piattaforma open source per la configurazione e la gestione grafica di centralini telefonici basati su Asterisk (stima di impatto sistemico **79,48/100**). Link all'alert del 29/08/2025;
  - **Adobe:** rilasciati aggiornamenti di sicurezza per risolvere due vulnerabilità, di cui una con gravità "alta" e una con gravità "critica", in Adobe Experience Manager Forms on Java Enterprise Edition (JEE). Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato remoto di eseguire codice arbitrario e/o la lettura di dati sui sistemi target (stima di impatto sistemico **79,48/100**). Link all'alert del 07/08/2025;
  - **Grafana Labs:** sanata una vulnerabilità con gravità "critica" in Grafana, nota applicazione web per la visualizzazione e l'analisi interattiva di dati. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di elevare i propri privilegi o di impersonificare altri utenti sui sistemi interessati, qualora configurati come indicato nel bollettino di sicurezza del vendor (stima di impatto sistemico **79,48/100**). Link all'alert del 20/11/2025;
  - **Cisco:** dopo gli avvisi di sicurezza diffusi di recente e trattati nell'ambito dell'alert AL01/250925/CSIRT-ITA, Cisco ha pubblicato ulteriori 4 vulnerabilità di sicurezza, di cui una con gravità "critica" e due zero-day sfruttate attivamente in rete. Nel dettaglio, le zero-day consentirebbero l'esecuzione di codice arbitrario e l'accesso a informazioni sensibili su prodotti Adaptive Security Appliance (ASA) e Firewall Threat Defense (FTD) vulnerabili (stima di impatto sistemico **79,35/100**). Link all'alert del 26/09/2025;
  - **Citrix:** rilevate 3 nuove vulnerabilità di sicurezza con gravità "critica" in Citrix NetScaler ADC e NetScaler Gateway (stima di impatto sistemico **79,35/100**). Link all'alert del 26/08/2025;
  - **Fortinet:** rilevate nuove vulnerabilità in molteplici prodotti Fortinet, di cui una con gravità "critica" e due con gravità "alta", presenti in FortiSIEM, FortiWeb, FortiOS, FortiPAM, FortiProxy e FortiSwitchManager (stima di impatto sistemico **79,23/100**). Link all'alert del 13/08/2025;
  - **Citrix:** in riferimento al AL05/250617/CSIRT-ITA, al fine di contrastare gli attacchi volti allo sfruttamento della vulnerabilità CVE-2025-5777 (nota anche col nome di "CitrixBleed 2"), questo CSIRT raccomanda a tutti i soggetti nazionali di procedere ad opportune verifiche e all'implementazione delle procedure di mitigazione (stima di impatto sistemico **79,23/100**). Link all'alert del 09/07/2025;
  - **Microsoft:** ha rilasciato aggiornamenti di sicurezza per 2 vulnerabilità che interessano il prodotto SharePoint, nota piattaforma di collaborazione e gestione file. Nel dettaglio, la CVE-2025-53770 risulta sfruttata attivamente in rete: causata dalla deserializzazione di dati non attendibili, consente a un attaccante remoto non autenticato di eseguire codice arbitrario sulle istanze target (stima di impatto sistemico **79,23/100**). Link all'alert del 21/07/2025;
  - **React Native Community:** disponibile un Proof of Concept (PoC) per la CVE-2025-11953, relativa al pacchetto NPM Cli, distribuito nell'ambito del progetto "React Native Community". Tale software gestisce la command-line interface di React Native, framework di sviluppo mobile JavaScript multiplatforma. La vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto l'esecuzione di comandi arbitrari sul sistema interessato (stima di impatto sistemico **79,23/100**). Link all'alert del 05/11/2025;
  - **Microsoft:** rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-59287 con gravità "critica" – già sanata dal vendor – relativa a Windows Server Update Service (WSUS), servizio di Microsoft che consente agli amministratori

- di sistema di gestire centralmente la distribuzione degli aggiornamenti software per i prodotti Microsoft all'interno di una rete aziendale. Tale vulnerabilità potrebbe consentire a un utente malevolo non autenticato di eseguire codice arbitrario remoto sui sistemi target (stima di impatto sistemico **79,23/100**). Link all>alert del 25/10/2025;
- **Fortinet:** rilevate nuove vulnerabilità in alcuni prodotti Fortinet, di cui una con gravità "critica" e una con gravità "alta" presenti in FortiWeb e FortiVoice (stima di impatto sistemico **78,97/100**). Link all>alert del 09/07/2025;
  - **Formbricks:** disponibile un Proof of Concept (PoC) per la CVE-2025-59934, che riguarda Formbricks, piattaforma open-source per sondaggi e gestione dell'esperienza utente. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di bypassare i normali meccanismi di autenticazione sui sistemi interessati (stima di impatto sistemico **78,71/100**). Link all>alert del 29/09/2025;
  - **Sudo project:** rilevate due vulnerabilità di sicurezza, di cui una con gravità "critica", in "sudo", nota utility per sistemi operativi Unix-like che permette di delegare i privilegi utente. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato di elevare i propri privilegi ed eseguire codice arbitrario sui sistemi target (stima di impatto sistemico **78,58/100**). Link all>alert del 01/07/2025;
  - **Gladinet:** ricercatori di sicurezza hanno rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-12480 che interessa il prodotto Gladinet TrioFox, soluzione di accesso remoto sicuro ai file server aziendali, progettate per modernizzare la gestione dei file senza richiedere la migrazione al cloud (stima di impatto sistemico **78,33/100**). Link all>alert del 13/11/2025;
  - **Google Chrome:** rilevato lo sfruttamento attivo in rete della vulnerabilità identificata dal codice Chrome Issue 466192044. Tale vulnerabilità, stando a quanto riportato, sfrutterebbe una impropria gestione della dimensione dei buffer, che potrebbe causare perdita di riservatezza ed esecuzione arbitraria di codice (stima di impatto sistemico **78,20/100**). Link all>alert del 11/12/2025;
  - **D-Link:** disponibili Proof of Concept (PoC) per lo sfruttamento di varie vulnerabilità presenti nel modello D-Link DIR-878. Specificamente riguardo alle CVE-2025-60672, CVE-2025-60673, CVE-2025-60674 e CVE-2025-60676 (stima di impatto sistemico **77,94/100**). Link all>alert del 19/11/2025;
  - **Cisco:** rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-20393, con gravità "critica", che interessa i prodotti Cisco Secure Email Gateway e Cisco Secure Email and Web Manager. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato remoto, non autenticato, di eseguire codice arbitrario sui i sistemi interessati (stima di impatto sistemico **77,94/100**). Link all>alert del 18/12/2025;
  - **ISC:** aggiornamenti di sicurezza ISC sanano due vulnerabilità con gravità "alta", nel prodotto BIND. Tali vulnerabilità, qualora sfruttate, potrebbero causare la manomissione della cache DNS e/o la compromissione della disponibilità del servizio (stima di impatto sistemico **77,69/100**). Link all>alert del 22/10/2025;
  - **Notepad++:** disponibile un Proof of Concept (PoC) per la CVE-2025-56383, che riguarda Notepad++, noto editor di testo avanzato per Windows. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di eseguire codice arbitrario sui sistemi target (stima di impatto sistemico **77,56/100**). Link all>alert del 29/09/2025;
  - **PHP:** aggiornamenti di sicurezza sanano 3 nuove vulnerabilità in PHP, noto interprete del linguaggio di scripting per lo sviluppo web (stima di impatto sistemico **77,17/100**). Link all>alert del 07/07/2025;
  - **Gladinet:** ricercatori di sicurezza hanno rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-11371 che interessa i prodotti Gladinet CentreStack e TrioFox, soluzioni di accesso remoto sicuro ai file server aziendali, progettate per modernizzare la gestione dei file senza richiedere la migrazione al cloud (stima di impatto sistemico **77,05/100**). Link all>alert del 10/10/2025;
  - **VMware:** rilasciati aggiornamenti di sicurezza per sanare diverse vulnerabilità con gravità "alta", tra cui una 0-day, presenti nelle componenti NSX, vCenter, Cloud Foundation Operations, Aria Operations e Tools, utilizzate in diversi

prodotti VMware (stima di impatto sistemico **76,66/100**). Link all’alert del 30/09/2025;

### 3.2 Distribuzione delle vulnerabilità sui vendor

In Figura 7 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor.

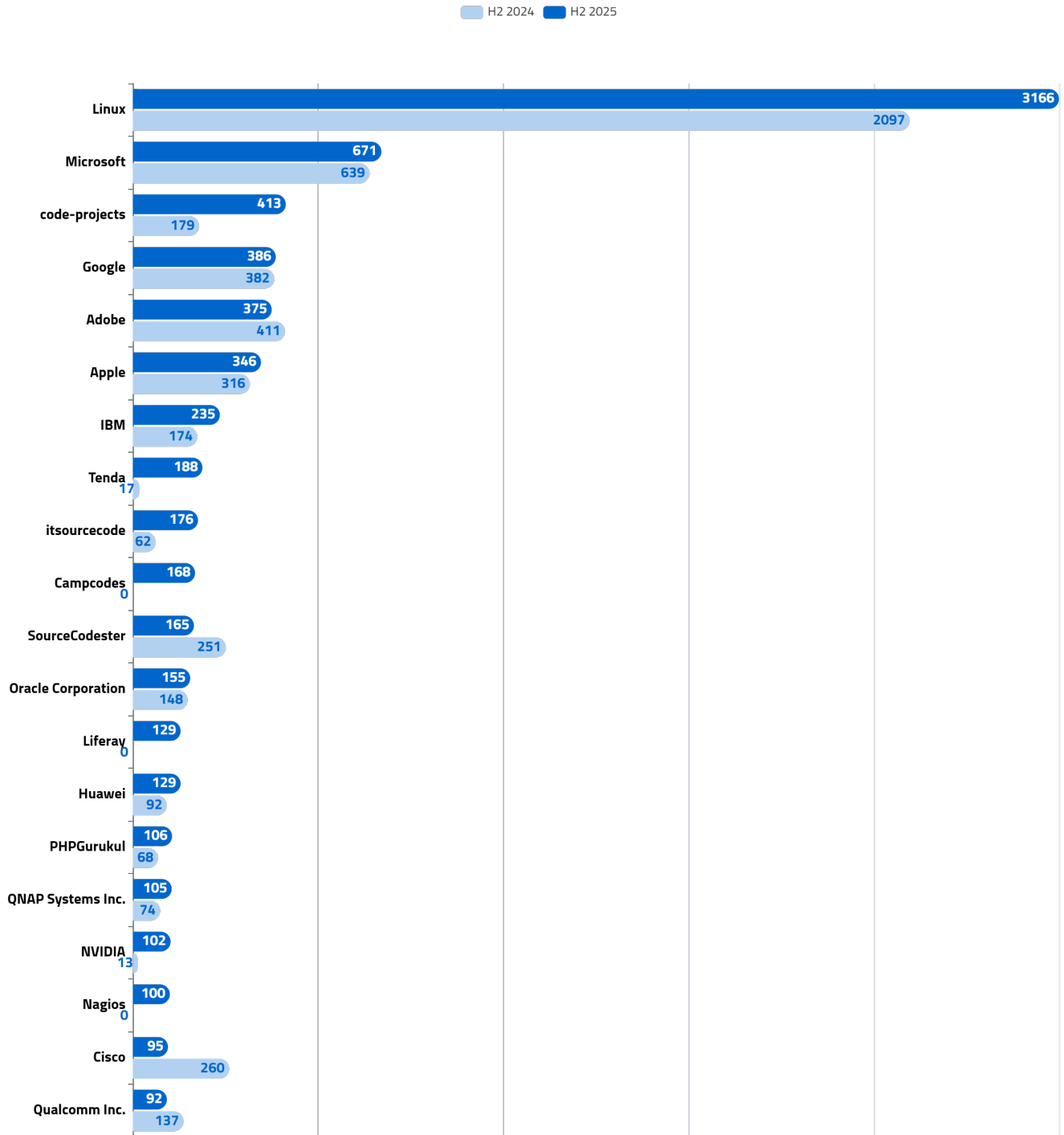


Figura 7 - top 20 produttori affetti da vulnerabilità nel II semestre 2025 e II semestre 2024

In Figura 8 è riportato, invece, il numero delle vulnerabilità rilevate distribuite tra i principali prodotti.

H2 2024 H2 2025

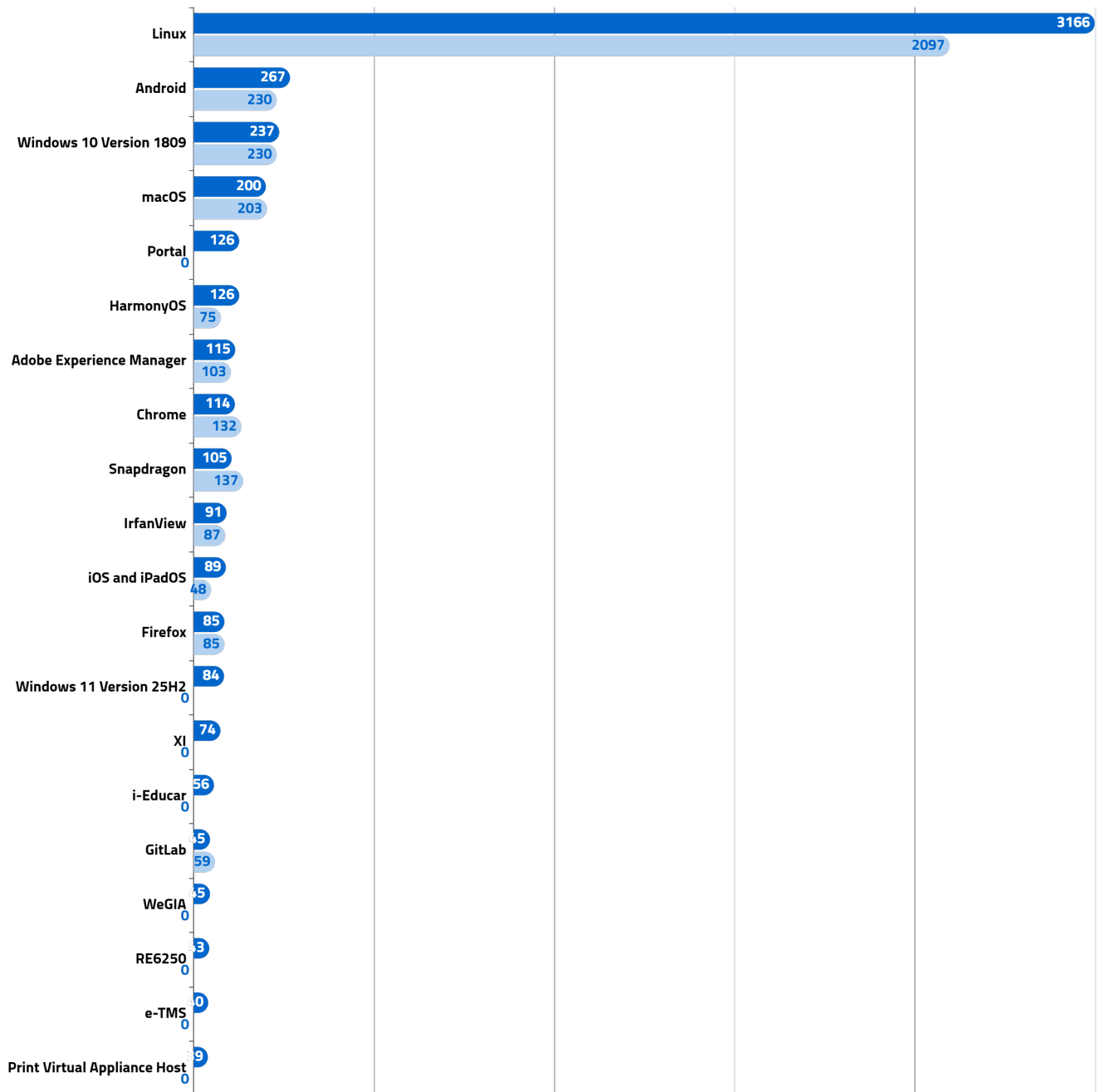


Figura 8 - top 20 prodotti affetti da vulnerabilità nel II semestre 2025 e II semestre 2024

### 3.3 CWE nel II semestre 2025

In Figura 9 sono riportate le 10 tipologie di weakness (Common Weakness Enumeration – CWE) più rilevate.

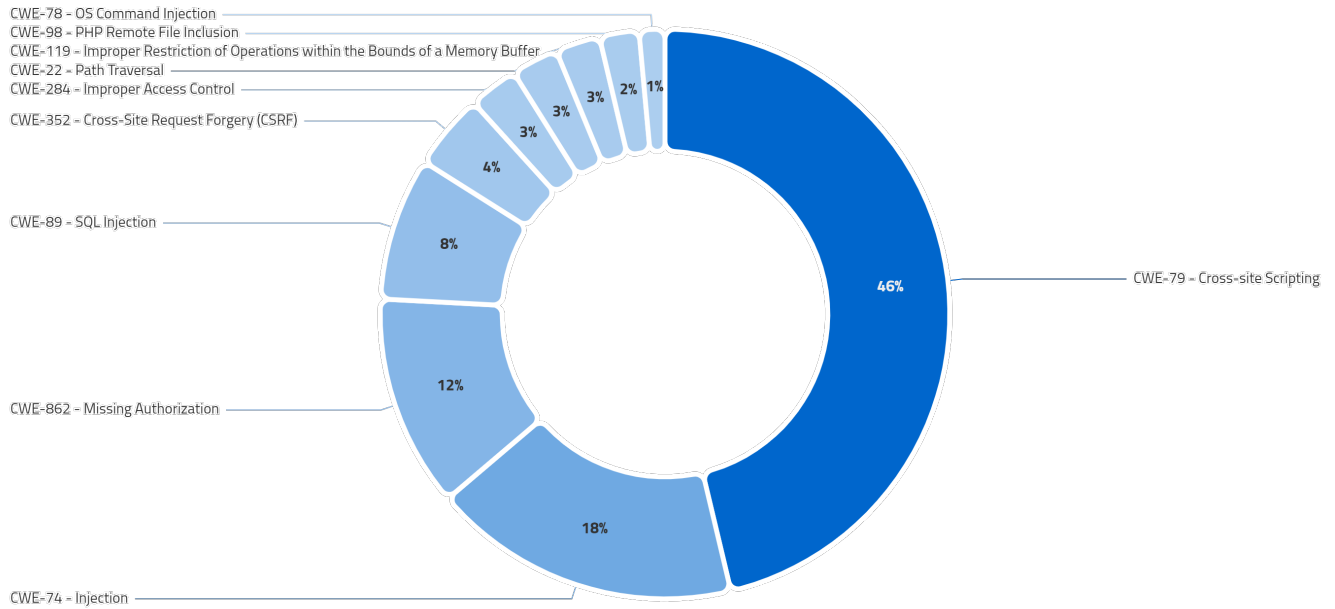


Figura 9 - top 5 CWE nel II semestre 2025

# 4 MINACCIA

In questa sezione si riporta un dettaglio sulle minacce ransomware e DDoS, anche in termini di rivendicazioni effettuate dai gruppi hacker in Italia ed UE, mentre per il malware uno spaccato sul numero degli IoC<sup>7</sup> condivisi dal CSIRT Italia tramite piattaforma MISP<sup>8</sup>, in modo da caratterizzarne le tipologie più frequenti.

## 4.1 Ransomware: distribuzione delle vittime

Nel II semestre 2025, solo l'1% degli incidenti ransomware ha interessato soggetti critici, mentre il 19% ha riguardato soggetti a media criticità; la restante parte (80%) ha colpito soggetti non critici. Tale distribuzione conferma l'orientamento prevalente degli attori ransomware verso obiettivi meno strutturati e caratterizzati da limitate capacità di cybersicurezza.

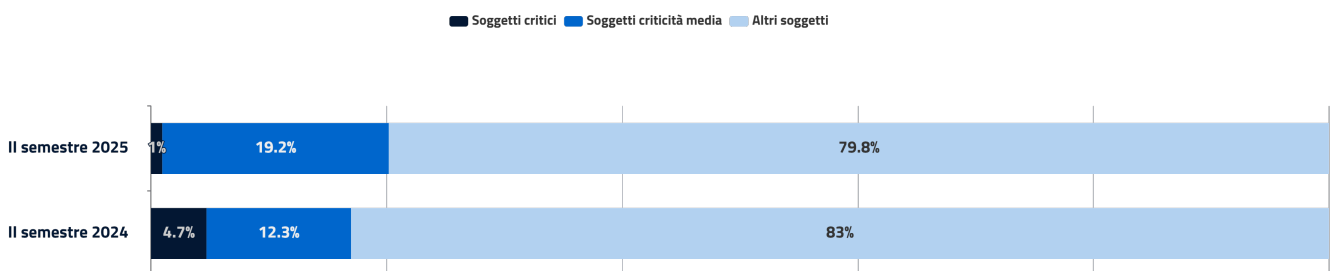


Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità

<sup>7</sup>IoC (Indicatore di Compromissione), indica la possibile presenza di un'attività malevola o un'intrusione nel sistema informatico. Gli IoC sono prove che gli analisti di sicurezza informatica utilizzano per identificare, rilevare e rispondere a una compromissione.

<sup>8</sup>MISP (Malware Information Sharing Platform) è una soluzione software open source per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce cyber.

## 4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel II semestre 2025 ha permesso di individuare **82** rivendicazioni di attacchi ransomware a danno di soggetti italiani<sup>9</sup>.

Il grafico in Figura 11 mostra l'andamento delle rivendicazioni nel corso degli ultimi 12 mesi.

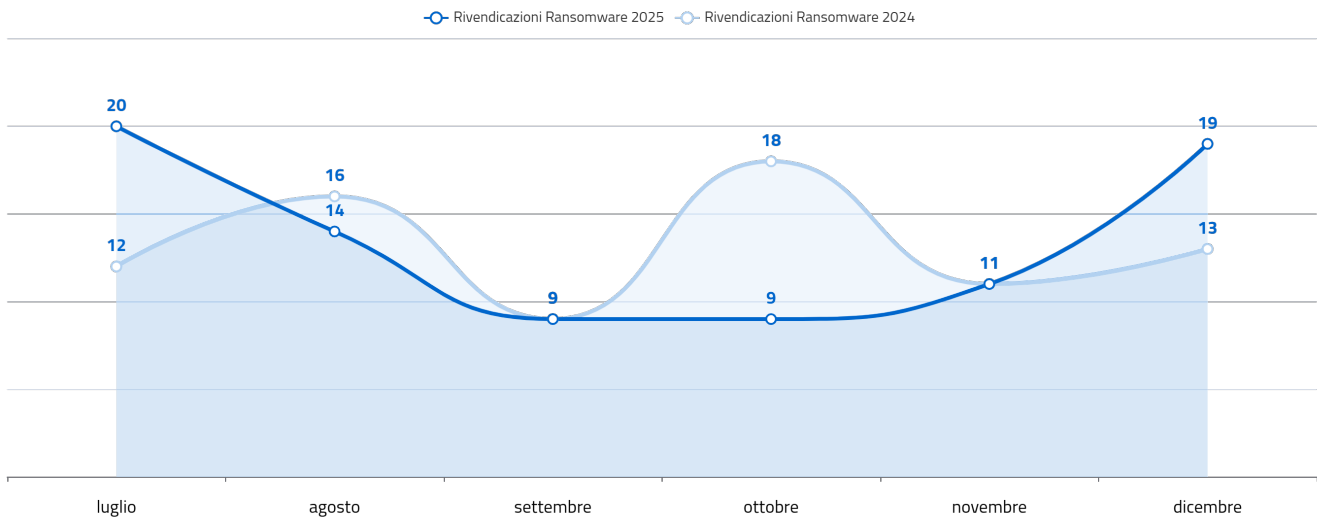


Figura 11 - *andamento delle rivendicazioni Ransomware*

Il grafico in Figura 12 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

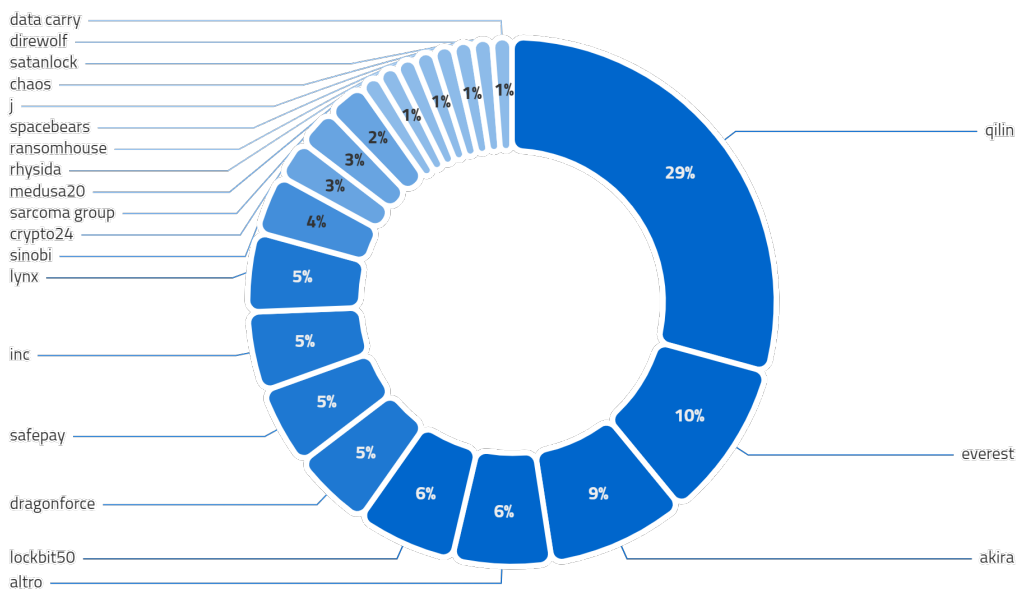


Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

<sup>9</sup>Talvolta, le rivendicazioni relative ad attacchi ransomware non sono confermate dal soggetto coinvolto.

### 4.3 Rivendicazioni DDoS

Nel II semestre 2025 sono state individuate<sup>10</sup> **202** rivendicazioni di attacchi DDoS in danno di soggetti italiani.

Il grafico in Figura 13 mostra l'andamento delle rivendicazioni DDoS nel corso del II semestre 2025 e del II semestre 2024.

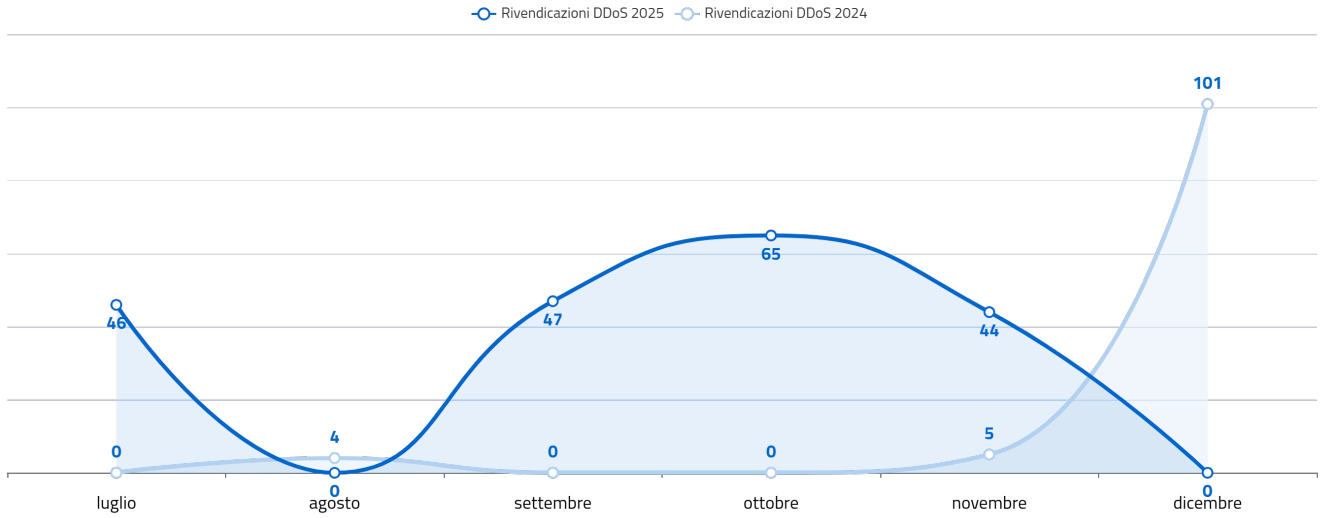


Figura 13 - andamento delle rivendicazioni DDoS

Il grafico in Figura 14 mostra i gruppi più attivi in termini di rivendicazioni.

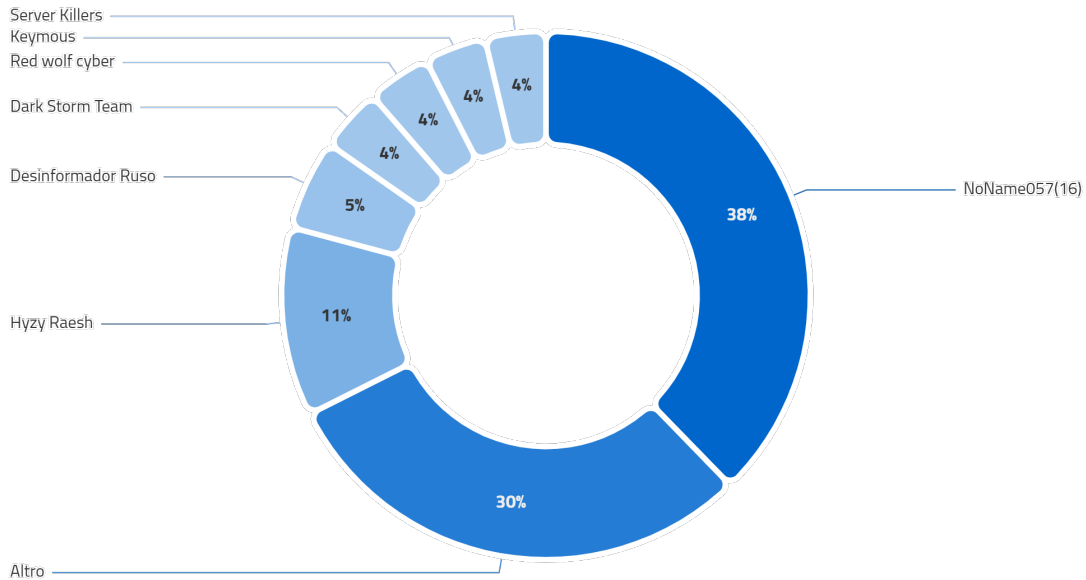


Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni

<sup>10</sup>I dati rappresentano solo gli eventi pubblicamente rivendicati.

# 5 MONITORAGGIO

L'ACN porta avanti attività di monitoraggio proattivo al fine di individuare e segnalare tempestivamente ai soggetti della constituency l'esposizione a specifiche criticità, che possono essere sfruttate, o che sono già in corso di sfruttamento. A valle dell'individuazione di tali criticità, il CSIRT Italia contatta i soggetti a rischio e, qualora risultino particolarmente diffuse, svolge opera di condivisione degli alert, sia tramite portale pubblico che attraverso i canali social dedicati (X, Telegram).

Durante il II semestre 2025 sono stati segnalati:

- **927 indirizzi web di phishing**, ovvero pagine web artefatte, contenenti riferimenti espliciti o simili a pagine web di circa **185** soggetti pubblici o privati della constituency, presumibilmente utilizzate per ingannare gli utenti e carpire credenziali;
- **5.904 dispositivi o servizi IT potenzialmente compromessi**, ovvero per i quali è stato rilevato un comportamento associabile a un'attività malevola in corso. Relativamente a tali dispositivi o servizi sono state inviate **4.704** comunicazioni, di cui il **12%** verso soggetti pubblici e **88%** verso soggetti privati;
- **12.534 dispositivi o servizi IT che espongono potenziali rischi**, come ad esempio versioni di software vulnerabili, per i quali sono state inviate **5.052** comunicazioni. Di queste il **31%** verso soggetti pubblici e **69%** verso soggetti privati.

Con particolare riguardo a quest'ultima fattispecie, risulta di interesse soffermarsi sia sulle categorie di dispositivi e servizi maggiormente esposti al pericolo di sfruttamento delle vulnerabilità, sia sulle tipologie di vulnerabilità da cui origina tale rischio. Raggruppando i dispositivi e servizi a rischio segnalati per categorie (Figura 15), si evince come tra le categorie più esposte al pericolo vi sia quella delle tecnologie per il lavoro remoto (principalmente *Virtual Private Network* e *Virtual Desktop*). Ciò è dovuto non solo al numero di vulnerabilità gravi emerse nell'ultimo anno su tali dispositivi, ma anche alla loro maggiore intrinseca esposizione ai rischi, in quanto devono essere raggiungibili direttamente tramite Internet per consentire l'accesso da remoto degli utenti.

Il grafico in figura 15 riporta il numero di asset a rischio segnalati suddivisi per categoria (top 10).

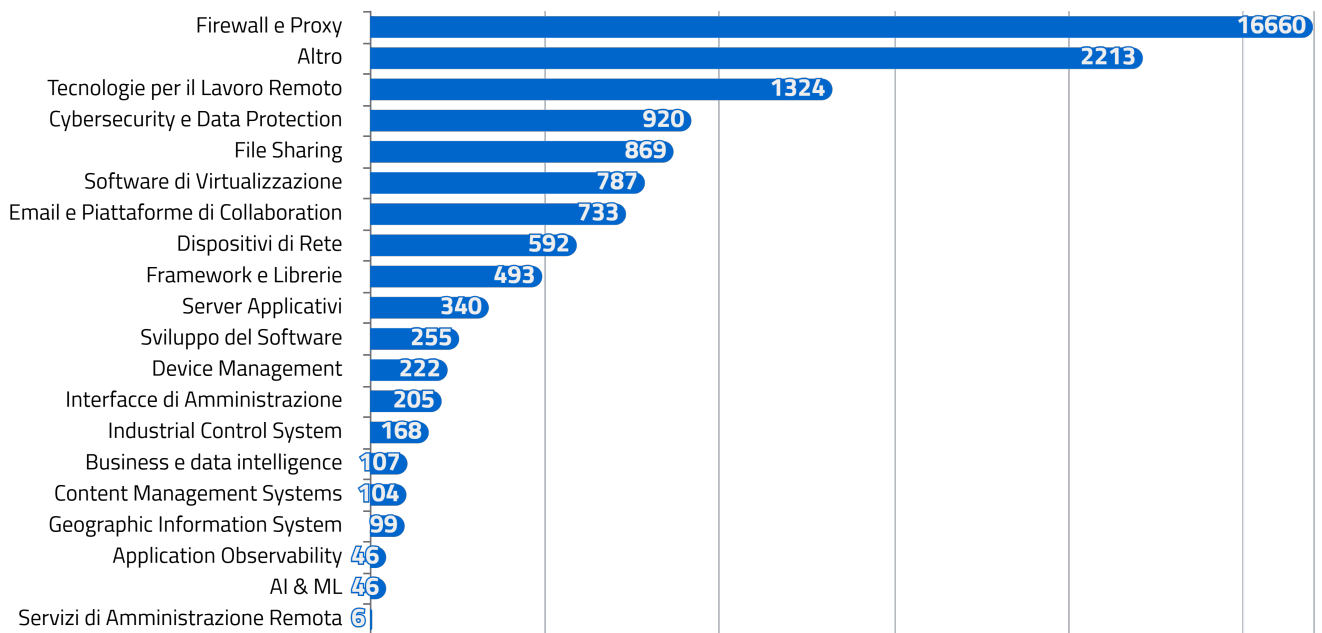


Figura 15 - Numero di asset a rischio segnalati suddivisi per categoria

Nella figura 16, invece, gli asset a rischio sono divisi a seconda delle tipologie di vulnerabilità, rinvenute e segnalate ai soggetti, con la relativa specificità del livello di gravità.

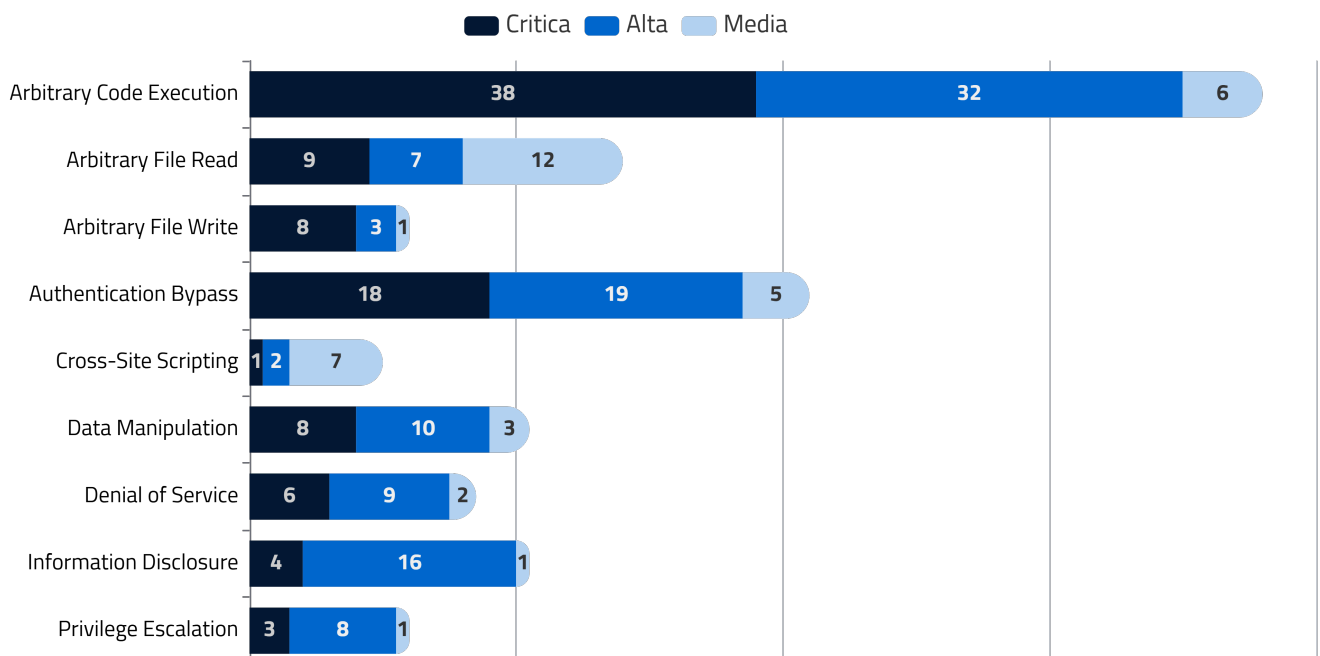


Figura 16 - Tipologia e gravità delle vulnerabilità rinvenute e segnalate negli asset a rischio

## 5.1 Comunicazioni dirette

Nel II semestre 2025 sono state diramate un totale di **5.205** comunicazioni verso i soggetti della constituency che espongono pubblicamente su Internet complessivamente **15.360** servizi a rischio. In Figura 17 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto e di seguito si riportano i dettagli e i link agli alert (ove presenti) delle campagne di comunicazione di allertamento svolte dal CSIRT Italia nei vari mesi, evidenziando il prodotto interessato.

In Figura 17 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto.

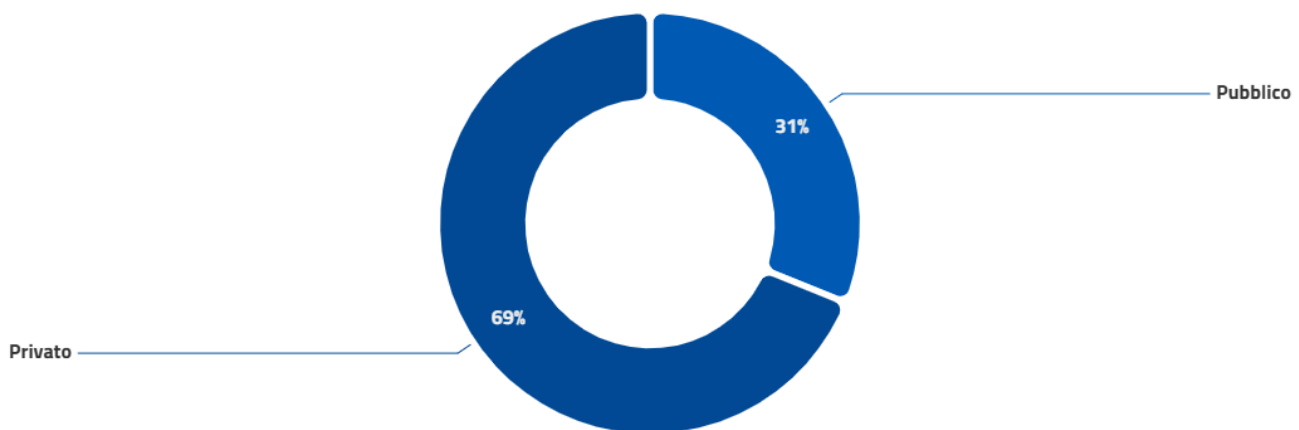


Figura 17 - distribuzione delle segnalazioni per tipologia di soggetto

## Luglio

- **Microsoft SharePoint** (CVE-2025-53771, CVE-2025-53770): tali vulnerabilità - zero-day e rispettivamente di tipo *Remote Code Execution* e *Spoofing* - causate dalla deserializzazione di dati non attendibili e la mancata validazione del pathname, darebbero vita alla catena di sfruttamento denominata "ToolShell" che consentirebbe a un attaccante remoto non autenticato di eseguire codice arbitrario sulle istanze target effettuando spoofing nella rete. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2025-49701, CVE-2025-49706): tali vulnerabilità - rispettivamente di tipo *Remote Code Execution* e *Spoofing* - consentirebbero a un attaccante autenticato e con i privilegi di almeno di *Site Owner* di eseguire codice arbitrario da remoto (CVE-2025-49701) e di impersonare un utente legittimo o un servizio (CVE-2025-49706), tramite la manipolazione degli header HTTP o dei token di autenticazione ed eludendo i controlli di accesso, permettendo l'accesso a file sensibili. Inoltre, quest'ultima vulnerabilità - laddove combinata con la CVE-2025-49704 - permetterebbe di ottenere una catena di exploit (denominata *ToolShell*) la quale consentirebbe di ottenere un accesso non autorizzato ai sistemi impattati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Citrix** (CVE-2025-6543, CVE-2025-5777): in particolare:
  - la CVE-2025-5777 (denominata *CitrixBleed 2*) – di tipo *Out-of-bounds Read* – consentirebbe a un eventuale attaccante non autenticato di accedere a dati potenzialmente sensibili presenti nella memoria dei sistemi affetti,

sfruttando un'errata validazione dell'input (*Memory Overread*), laddove essi siano configurati come Gateway (ad esempio VPN virtual server, ICA Proxy, CVPN, RDP Proxy) oppure come AAA virtual server;

- La CVE-2025-6543 – di tipo *Buffer Overflow* – infine, potrebbe consentire a un eventuale attaccante eludere il normale di esecuzione e di indurre il dispositivo in una condizione di Denial of Service.

Ulteriori dettagli negli alert relativi alle CVE-2025-5777 e CVE-2025-5349 (alert) e alla CVE-2025-6543 (alert) sul sito dello CSIRT Italia.

- **Fortinet FortiWEB** (CVE-2025-25257): tale vulnerabilità - di tipo *SQL Injection* - consentirebbe a un attaccante remoto non autenticato di eseguire codice o comandi SQL attraverso richieste HTTP(S) opportunamente predisposte. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **VMware (Cloud Foundation ESX, vSphere Foundation ESX, ESXi, Workstation, Fusion, Cloud Foundation, Telco Cloud Platform, Telco Cloud Infrastructure e VMware Tools)** (CVE-2025-41236): tale vulnerabilità – nel driver di rete virtuale VMXNET3 e di tipo *Integer Overflow* (Out-of-bounds Write) – consentirebbe ad un attaccante con privilegi amministrativi locali su una macchina virtuale che utilizza questo adattatore di eseguire codice sul sistema *host* violando l'isolamento tra VM (sistema *guest*) e *host*. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Node.js** (CVE-2025-27209, CVE-2025-27210): tali vulnerabilità consentirebbero a un eventuale attaccante di eseguire, rispettivamente, attacchi di tipo *HashDoS* (Hash Denial of Service) tramite l'invio di stringhe opportunamente predisposte - generando collisioni di hash e causando rallentamenti gravi o blocchi dell'applicazione affette - e l'accesso a file sensibili (come file di configurazioni o credenziali) tramite tecniche di *Path Traversal*, eludendo i meccanismi di protezione della funzione *path.normalize*, limitatamente a sistemi Windows che facciano uso della funzione *path.join* e a nomi di dispositivo Windows (come *CON*, *PRN* e *AUX*). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Wing FTP Server** (CVE-2025-47812): tale vulnerabilità – di tipo *Code Injection* – consentirebbe a un attaccante autenticato come utente anonimo (*anonymous*) di iniettare all'interno dei file di sessione utente codice Lua arbitrario e di eseguirlo a causa di una gestione errata dei byte "NULL" presenti nel parametro username da parte del sistema affetto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ivanti Endpoint Manager Mobile (EPMM)** (CVE-2025-6771 e CVE-2025-6770): tali vulnerabilità - di tipo *OS Command Injection* - qualora sfruttate, permetterebbero ad un utente malintenzionato autenticato con privilegi elevati l'esecuzione remota di codice arbitrario sui dispositivi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **AMI MegaRAC** (CVE-2024-54085): tale vulnerabilità - di tipo *Authentication Bypass* - potrebbe consentire a un attaccante di eludere i meccanismi di autenticazione tramite l'invio di una richiesta HTTP opportunamente predisposta - sfruttando l'header HTTP "X-Server-Addr", mediante il quale il *Baseboard Management Controller* (BMC) identifica le richieste "host-trusted" - al fine di ottenere il pieno accesso ai comandi del BMC sui sistemi affetti, con impatti su riservatezza, integrità e disponibilità dei sistemi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Redis** (CVE-2025-32023): tale vulnerabilità – di tipo *Buffer Overflow* – permetterebbe, tramite l'invio di dati opportunamente predisposti, a un eventuale attaccante autenticato di effettuare operazioni di scrittura oltre i limiti del buffer (heap o stack) sulla porzione di memoria riservata alle operazioni *HyperLogLog* e di eseguire potenzialmente codice arbitrario da remoto sui sistemi Redis affetti aventi tale funzionalità implementata.
- **Open Source Geospatial Foundation GeoServer** (CVE-2024-29198): tale vulnerabilità – di tipo *Server-Side Request Forgery* – consentirebbe a un eventuale attaccante non autenticato di enumerare le reti interne del server e, in caso di istanze nel cloud, di ottenere dati sensibili dell'organizzazione sfruttando una servlet (*TestWfsPost*) nella

- funzionalità di demo (Demo request endpoint) qualora la proprietà Proxy Base URL non fosse impostata.
- **CrushFTP** (CVE-2025-54309): tale vulnerabilità – zero-day e di tipo *Authentication Bypass* – potrebbe consentire a un attaccante remoto di ottenere accesso amministrativo ai sistemi affetti tramite l’invio di una richiesta HTTPS opportunamente predisposta, violando la validazione del protocollo AS2 (utilizzato per lo scambio sicuro di dati via HTTPS). Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **Oracle WebLogic Server** (CVE-2025-30762): tale vulnerabilità – di tipo *Authentication Bypass* – consentirebbe a un eventuale attaccante non autenticato e con accesso di rete al sistema affetto mediante i protocolli T3/IIOP di accedere a dati sensibili senza bisogno di credenziali o interazione utente eludendo i meccanismi di autenticazione. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **XWiki** (CVE-2025-32429): tale vulnerabilità – di tipo *SQL Injection* – potrebbe permettere a un eventuale attaccante, tramite opportuna manipolazione del parametro *sort* del file *getdeleteddocuments.vm*, di eludere i meccanismi di sicurezza sui sistemi target e di accedere a dati sensibili o di modificarne il contenuto per mezzo di codice SQL malevolo, inserendo il valore direttamente nella clausola ‘ORDER BY’ senza alcuna validazione. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **Cisco (Identity Services Engine (ISE) e Cisco ISE Passive Identity Connector** (CVE-2025-20337): tale vulnerabilità – di tipo *Code Injection* – consentirebbe a un eventuale attaccante, tramite una richiesta API opportunamente predisposta, di ottenere l’accesso al dispositivo vulnerabile con privilegi massimi (root) e di eseguire codice arbitrario con tali privilegi. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **Cisco Unified Communications Manager** (CVE-2025-20309): tale vulnerabilità – di tipo *Authentication Bypass* – consentirebbe ad un attaccante remoto malintenzionato di accedere ai dispositivi affetti tramite l’utente “root” sfruttando credenziali statiche di sviluppo (hardcoded) che non possono essere cambiate né eliminate. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **Atlassian Jira Data Center e Server** (CVE-2025-22157): tale vulnerabilità – di tipo *Privilege Escalation* – potrebbe consentire a un utente malintenzionato per elevare da remoto i propri privilegi sui sistemi affetti.
  - **PaperCut NG/MF** (CVE-2023-2533): tale vulnerabilità – di tipo *Cross-Site Request Forgery* – consentirebbe a un attaccante remoto in possesso di una sessione utente di tipo amministratore di eseguire codice arbitrario sui sistemi affetti. Ciò sarebbe possibile, ad esempio, inducendo un amministratore con sessione attiva sull’interfaccia di amministrazione del prodotto in oggetto, a cliccare su un link malevolo opportunamente predisposto, alterando così le configurazioni di sicurezza e/o eseguendo codice arbitrario. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

---

## Agosto

- **Citrix NetScaler e Gateway** (CVE-2025-7775): tale vulnerabilità – di tipo *Memory Overflow* – consentirebbe a un eventuale attaccante non autenticato, tramite l’invio di richieste HTTP/QUIC/SSL opportunamente predisposte, di sovrascrivere porzioni di memoria nelle installazioni affette, eseguendo codice arbitrario da remoto con i privilegi del processo NetScaler e interruzioni del servizio (DoS). Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **SonicWall Firewall** (CVE-2024-40766): tale vulnerabilità – di tipo *Improper Access Control* – consentirebbe a un eventuale attaccante, anche qualora siano abilitate soluzioni multi-fattore (MFA), di eludere i meccanismi di autenticazione sui sistemi affetti aventi la funzionalità SSLVPN attiva. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

- **Squid** (CVE-2025-54574): tale vulnerabilità – di tipo *Heap Buffer Overflow* – potrebbe consentire a un attaccante senza privilegi e autenticazione di sovrascrivere la porzione di memoria dell'heap utilizzata dall'applicativo per il contenimento delle richieste URN (Uniform Resource Name) tramite l'invio di richieste HTTP opportunamente predisposte, permettendogli di eseguire codice arbitrario da remoto, causare un Denial-of-Service (DoS) e potenzialmente ottenere informazioni sensibili (come credenziali) dalla memoria acceduta. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **SonicWall SMA100 series** (CVE-2025-40598, CVE-2025-40597, CVE-2025-40596): tali vulnerabilità – rispettivamente di tipo *Stack Based Buffer Overflow*, *Heap Based Buffer Overflow* e *Cross-Site Scripting* – potrebbero consentire a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario e/o compromettere la disponibilità del servizio sui sistemi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Microsoft Exchange** (CVE-2025-53786): tale vulnerabilità – di tipo *Elevation of Privilege* – potrebbe consentire a un attaccante con accesso amministrativo su un server Exchange locale di sfruttare un meccanismo di autenticazione condiviso per elevare i privilegi utente ed effettuare accessi non autorizzati a Exchange Online senza generare alcuna evidenza nei log ed eludendo i controlli di sicurezza. Ciò sarebbe possibile negli ambienti Exchange Server affetti da tale problematica e configurati in modalità "ibrida", ovvero aventi componenti sia on-premises che cloud. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Salesforce Tableau Server** (CVE-2025-26496): tale vulnerabilità – di tipo *Type Confusion* – consentirebbe, tramite il caricamento di un file opportunamente predisposto e sfruttando la gestione errata dei tipi di dati da parte dell'applicazione, a un attaccante non autenticato di eseguire codice arbitrario da remoto, accedere a file e dati sensibili e il caricamento di artefatti malevoli, compromettendo i sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Mitel MiCollab** (CVE-2025-52914): tale vulnerabilità - di tipo *SQL injection* - consentirebbe a un attaccante autenticato di accedere a dati sensibili, modificare o cancellare informazioni e compromettere la disponibilità del sistema mediante comandi SQL sfruttando un'insufficiente validazione dell'input da parte del modulo "Suite Applications Services" (responsabile della gestione delle richieste web e dell'interazione con il database). Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Directus** (CVE-2025-55746): tale vulnerabilità - di tipo *Unrestricted Upload of File with Dangerous Type* - potrebbe consentire a un utente malintenzionato non autenticato e in possesso di almeno un asset UUID valido di modificare file esistenti o di creare file arbitrari sui sistemi target. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Commvault CommCell** (CVE-2025-57789, CVE-2025-57790, CVE-2025-57791, CVE-2025-57788): tali vulnerabilità - di tipo "Remote Code Execution" e "Authentication Bypass" - qualora sfruttate, potrebbero permettere a un utente malintenzionato remoto l'esecuzione di codice arbitrario e il bypass dei meccanismi di autenticazione sui dispositivi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Plex Media Server** (CVE-2025-34158): tale vulnerabilità - di tipo *Improper Input Validation* - è dovuta ad una non corretta verifica dei dati forniti dall'utente prima dell'utilizzo. Questo può portare a comportamenti imprevisti, sfruttabili da un utente malintenzionato. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2025-53771, CVE-2025-53770): tali vulnerabilità - rispettivamente di tipo *Remote Code Execution* e *Spoofing* - causate dalla deserializzazione di dati non attendibili e la mancata validazione del "pathname", consentirebbero a un attaccante remoto non autenticato di eseguire codice arbitrario sulle istanze target effettuando spoofing nella rete. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Adobe Experience Manager** (CVE-2025-54254, CVE-2025-54253): tali vulnerabilità – rispettivamente di tipo *Misconfiguration* e *XML External Entity Reference (XXE) Injection* – qualora sfruttate, potrebbero consentire a un

- utente malintenzionato remoto di eseguire codice arbitrario (CVE-2025-54253) – tramite bypass dei meccanismi di autenticazione e utilizzo della modalità sviluppatore di Apache Struts2 – e la lettura di file arbitrari – anche sensibili – sui sistemi target (CVE-2025-54254). Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **N-able N-central** (CVE-2025-8876, CVE-2025-8875): tali vulnerabilità - di tipo rispettivamente *Deserialization of Untrusted Data* e *OS Command Injection* - potrebbero permettere a un attaccante autenticato di eseguire codice arbitrario ed elevare i propri privilegi sui sistemi affetti. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
  - **Samsung magicINFO 9** (CVE-2025-54451): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante non autenticato di eseguire codice arbitrario da remoto. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

## Settembre

- **Cisco Adaptive Security Appliance, Cisco Firewall Threat Defense, Cisco IOS, Cisco IOS XE e Cisco IOS XR** (CVE-2025-20363, CVE-2025-20362 e CVE-2025-20333): le vulnerabilità identificate tramite le CVE-2025-20333 e CVE-2025-20363 - rispettivamente di tipo *Classic Buffer Overflow* e *Heap-Based Buffer Overflow* - consentirebbero a un attaccante autenticato l’esecuzione di codice arbitrario da remoto con privilegi elevati, tramite l’invio di richieste HTTP(S) opportunamente predisposte. La terza vulnerabilità, identificata tramite la CVE-2025-20362 - di tipo *Missing Authorization* - consentirebbe invece l’accesso a URL riservate eludendo i meccanismi di autenticazione, sfruttando una non corretta validazione dei parametri di input. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia (consultare anche l’alert specifico sullo sfruttamento delle due vulnerabilità zero-day).
- **Cisco IOS e Cisco IOS XE** (CVE-2025-20352): tale vulnerabilità - di tipo *Stack-Based Buffer Overflow* - relativa alla componente SNMP di Cisco IOS e IOS XE, consentirebbero a un attaccante remoto autenticato, tramite l’invio di pacchetti SNMP appositamente predisposti e a seconda dei privilegi posseduti, di causare una interruzione del servizio o l’esecuzione di codice arbitrario da remoto. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Formbricks** (CVE-2025-59934): tale vulnerabilità – di tipo *Improper Authentication* – potrebbe consentire a un eventuale attaccante in possesso di uno “user.id” di un dato utente di forgiare un *JSON Web Token (JWT)* per bypassare i normali meccanismi di autenticazione per l’utente e richiedere il reset della password di quest’ultimo. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Ivanti Connect Secure** (CVE-2025-55144, CVE-2025-55143, CVE-2025-55142, CVE-2025-55141, CVE-2025-55139, CVE-2025-55148, CVE-2025-55147, CVE-2025-55146, CVE-2025-55145, CVE-2025-8711 e CVE-2025-8712): tali vulnerabilità - di tipo *Missing Authorization*, *Cross-Site Request Forgery (CSRF)*, *Unchecked Return Value*, *Server-Side Request Forgery (SSRF)* e *Cross-site Scripting (XSS)* - potrebbero consentire a un attaccante di esfiltrare credenziali e dati di sessione, inviare richieste interne al sistema per attività di ricognizione, condurre attacchi di tipo Denial of Service ai sistemi impattati, intercettare o manipolare sessioni (HTML5) attive, accedere e modificare configurazioni sensibili potenzialmente ottenendo privilegi elevati e - in presenza di interazione utente - l’esecuzione di azioni - anche privilegiate - per il conto di quest’ultimo. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Django** (CVE-2025-57833): tale vulnerabilità - di tipo *SQL Injection* - potrebbe consentire a un attaccante remoto non autenticato di inviare un input malevolo interpretato direttamente nelle dalle motore SQL portando potenzialmente all’accesso non autorizzato ai dati, alla modifica e/o cancellazione di informazioni e all’esecuzione di comandi arbitrari sul database relativo al backend dell’applicazione web. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

- **Sangoma FreePBX** (CVE-2025-57819): tale vulnerabilità - di tipo *Authentication Bypass* - permetterebbe a un attaccante non autenticato, attraverso lo sfruttamento di una non corretta sanitizzazione degli input forniti al modulo endpoint, di accedere all'interfaccia di amministrazione del prodotto (FreePBX Administration) e potenzialmente effettuare modifiche sul database o eseguire codice arbitrario da remoto sui sistemi impattati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **GitLab** (CVE-2025-6454): tale vulnerabilità - di tipo *Server-Side Request Forgery (SSRF)* - consentirebbe ad un utente autenticato di inviare richieste appositamente predisposte, attraverso ambienti proxy, allo scopo di eseguire richieste non previste. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **SAP Netweaver** (CVE-2025-42958, CVE-2025-42922 e CVE-2025-42944): In particolare, tali vulnerabilità - rispettivamente di tipo *Deserialization of Untrusted Data*, *Code Injection* e *Execution with Unnecessary Privileges* - potrebbero consentire a un attaccante di eseguire da remoto comandi arbitrari sul sistema operativo - anche in assenza di autenticazione - (CVE-2025-42944) - di caricare file arbitrari e di eseguirli (CVE-2025-42922) e di accedere a funzionalità amministrative o di leggere/modificare/eliminare informazioni sensibili (CVE-2025-42958) - laddove sia in possesso di credenziali valide. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Digiever NVR** (CVE-2025-10265, CVE-2025-10264): tali vulnerabilità - rispettivamente di tipo *OS Command Injection* e *Information Disclosure* - potrebbero consentire a un attaccante non autenticato di iniettare comandi arbitrari al sistema operativo del dispositivo impattato tramite l'invio di richieste HTTP opportunamente predisposte e di ottenere l'accesso - anche in modifica - al file di configurazione. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **WatchGuard Firewall** (CVE-2025-9242): la vulnerabilità - di tipo *Out-of-bounds Write* - qualora sfruttata, potrebbe consentire a un eventuale attaccante non autenticato di eseguire da remoto codice arbitrario su dispositivi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **GoAnywhere MFT** (CVE-2025-10035): tale vulnerabilità - di tipo *Command Injection* - riguarda le modalità di deserializzazione da parte del License Servlet e, qualora sfruttata, potrebbe consentire a un attaccante non autenticato di deserializzare un oggetto Java arbitrario da esso controllato e di iniettare comandi del sistema operativo, permettendogli così di eseguire da remoto codice arbitrario sui sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **FlowiseAI** (CVE-2025-58434): tale vulnerabilità - di tipo *Authentication Bypass* - potrebbe consentire a un attaccante di eludere i meccanismi di autenticazione sfruttando l'endpoint "forgot-password" che restituisce informazioni sensibili - incluso il Token valido per resettare la password per utenti arbitrari - senza alcuna verifica o autenticazione, portando ad una completa compromissione dell'account. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Omnissa Workspace ONE UEM** (CVE-2025-25231): tale vulnerabilità di tipo - *Path Traversal* - potrebbe consentire a un attaccante non autenticato l'accesso in sola lettura ad informazioni sensibili tramite l'invio di richieste GET opportunamente predisposte verso gli endpoint API. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Argo-CD** (CVE-2025-55190): tale vulnerabilità - di tipo *Exposure of Sensitive Information* - potrebbe consentire a un attaccante con permessi limitati, sfruttando l'API "/api/v1/projects/project/detailed/" dell'endpoint impattato, di esfiltrare dati sensibili, modificare il codice e compromettendo uno o più componenti o strumenti usati nel processo di sviluppo del codice. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **SolarWinds Web Help Desk** (CVE-2025-26399): tale vulnerabilità - di tipo *Deserialization of Untrusted Data* - relativa all'*AjaxProxy* potrebbe consentire a un attaccante non autenticato di eseguire codice arbitrario e comandi da remoto sui sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Progress OpenEdge** (CVE-2025-7388): tale vulnerabilità - di tipo *Command Injection* - potrebbe consentire ad un

utente malintenzionato autenticato di iniettare ed eseguire comandi del sistema operativo nel contesto del processo dell'AdminServer. Nello specifico, essa sarebbe stata sfruttata in combinazione con la CVE-2024-1403 - di tipo *Authentication Bypass* - al fine di ottenere l'esecuzione di codice da remoto anche in assenza di sessioni autenticate sui sistemi impattati da ambedue le vulnerabilità. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.

- **Ivanti Endpoint Manager Mobile** (CVE-2025-4428 e CVE-2025-4427): tali vulnerabilità - di tipo *Authentication Bypass* e *Remote Code Execution* - qualora sfruttate in maniera combinata, potrebbero consentire ad un utente malintenzionato remoto non autenticato il bypass dei meccanismi di autenticazione e l'esecuzione di codice arbitrario sui dispositivi target. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Moodle** (CVE-2023-30943): tale vulnerabilità - di tipo *Path Traversal* - che consentirebbe ad un attaccante remoto non autenticato la creazione arbitraria di cartelle, potrebbe essere sfruttata per eseguire un attacco di tipo *Stored Cross-Site Scripting (XSS)* nel pannello di amministrazione del sistema impattato, portando potenzialmente all'esecuzione di codice arbitrario da remoto.

---

## Ottobre

- **F5** (CVE-2025-53521, CVE-2025-53474, CVE-2025-48008, CVE-2025-46706 e CVE-2025-41430): tali vulnerabilità - di tipo *Denial of Service* e *Arbitrary Code Execution* - potrebbero consentire a un attaccante non autenticato il blocco del traffico di rete da remoto dei sistemi affetti - tramite l'invio pacchetti opportunamente predisposti - e la potenziale esecuzione di codice arbitrario, laddove l'attaccante disponga invece di un accesso in locale ai sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Apache Tomcat** (CVE-2025-55752 e CVE-2025-55574): tali vulnerabilità - rispettivamente di tipo *Improper Neutralization of Escape, Meta, or Control Sequences* e *Path Traversal* - permetterebbe a un eventuale attaccante di manipolare la visualizzazione dei log nella console, di eludere i meccanismi di sicurezza e/o di eseguire codice arbitrario da remoto sui sistemi impattati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration Suite** (CVE-2025-62763): tale vulnerabilità - di tipo *Server-Side Request Forgery (SSRF)* - potrebbe consentire a un'attaccante, tramite l'invio di richieste HTTP opportunamente predisposte e non correttamente validate dal modulo chat proxy di Zimbra, di accedere a risorse interne e dati sensibili. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **ISC BIND** (CVE-2025-40778): tale vulnerabilità - di tipo *Acceptance of Extraneous Untrusted Data With Trusted Data* - consentirebbe a un attaccante di iniettare dati nella cache tramite l'invio di *Resource Record* non richiesti, compromettendo potenzialmente la cache con un attacco di tipo *DNS Cache Poisoning*, capace di alterare la risoluzione dei nomi e reindirizzare gli utenti verso domini malevoli. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Libraesva Email Security Gateway** (CVE-2025-59689): tale vulnerabilità - di tipo *Command Injection* - potrebbe consentire a un attaccante, non autenticato, l'esecuzione di codice arbitrario da remoto sfruttando una non corretta sanitizzazione dei comandi durante la fase di analisi automatica, in ricezione della posta elettronica, degli allegati compressi. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Squid** (CVE-2025-62168): tale vulnerabilità - di tipo *Information Disclosure* - consentirebbe a un eventuale attaccante remoto di accedere a informazioni sensibili - come token di sicurezza e credenziali - utilizzate internamente dalle applicazioni web relative alle istanze affette. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **SAP Netweaver** (CVE-2025-42944): tali vulnerabilità - di tipo *Insecure Deserialization* - potrebbero consentire a un attaccante non autenticato l'esecuzione arbitraria da remoto di comandi sul sistema operativo, tramite l'invio di

- richieste appositamente predisposte verso il modulo RMI-P4. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cisco Adaptive Security Appliance (ASA), Firewall Threat Defense (FTD), IOS, IOS-XE, IOS-XR** (CVE-2025-20363, CVE-2025-20362 e CVE-2025-20333): le vulnerabilità identificate tramite le CVE-2025-20333 e CVE-2025-20363 - di tipo *Buffer Overflow* - consentirebbero a un attaccante autenticato l'esecuzione di codice arbitrario da remoto con privilegi elevati, tramite l'invio di richieste HTTP(s) opportunamente predisposte. La terza vulnerabilità identificata tramite la CVE-2025-20362 - di tipo *Missing Authorization* - consentirebbe invece l'accesso a URL riservate eludendo i meccanismi di autenticazione, sfruttando una non corretta validazione dei parametri di input.
  - **TP-Link Gateway Omada** (CVE-2025-7851, CVE-2025-7850, CVE-2025-6542 e CVE-2025-6541): tali vulnerabilità - di tipo *OS Command Injection* (CVE-2025-6541, CVE-2025-6542, CVE-2025-7850) e *Improper Privilege Management* (CVE-2025-7851) - qualora sfruttate, potrebbero consentire a un eventuale attaccante, anche non in possesso di credenziali valide, di eseguire comandi arbitrario da remoto sui sistemi operativi dei prodotti interessati e - in casi particolari - ottenere una shell come utente root. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Telerik UI** (CVE-2025-3600): tale vulnerabilità - di tipo *Unsafe Reflection* - potrebbe consentire a un attaccante, tramite l'invio di richieste HTTP opportunamente predisposte, di compromettere la disponibilità del servizio e/o di eseguire codice arbitrario da remoto sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Nagios Log Server** (CVE-2025-44824 e CVE-2025-44823): tali vulnerabilità - rispettivamente di tipo *Information Disclosure* e *Improper Authorization* - potrebbero consentire a un utente autenticato (anche non con privilegi di amministratore) di ottenere accesso alle chiavi API in chiaro di altri utenti (amministratori inclusi) sfruttando l'endpoint `/api/system/get_users` (CVE-2025-44823) e a un utente autenticato con permessi "read-only" di causare l'interruzione temporanea della disponibilità del servizio di logging, invocando l'endpoint `/api/system/stop?subsystem=elasticsearch` al fine di arrestare l'istanza Elasticsearch utilizzata dal prodotto (CVE-2025-44824). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Microsoft ASP.NET Core 8.0** (CVE-2025-55315): tale vulnerabilità - di tipo *HTTP Request/Response Smuggling* - e relativa a ASP.NET Core permetterebbe a un eventuale attaccante remoto di effettuare il bypass di meccanismi di sicurezza. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Ivanti Connect Secure** (CVE-2025-22457): tale vulnerabilità - di tipo *Stack-based Buffer Overflow* - potrebbe consentire a un eventuale attaccante non autenticato l'esecuzione di codice arbitrario da remoto sui dispositivi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Milesight** (CVE-2023-43261): tale vulnerabilità - di tipo *Insertion of Sensitive Information into Log File* - consentirebbe ad un eventuale attaccante di visualizzare file di log contenenti credenziali sensibili che potrebbero poi essere sfruttate per accedere all'interfaccia web, configurare VPN, disattivare firewall ed inviare SMS.
  - **Microsoft Windows Server Update Service** (CVE-2025-59287): tale vulnerabilità di tipo *Deserialization of Untrusted Data* - consentirebbe a un attaccante non autenticato, tramite l'invio di una richiesta opportunamente predisposta sulle porte TCP 8530/8531, una non corretta deserializzazione degli oggetti, permettendo l'esecuzione di codice arbitrario da remoto sui sistemi impattati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Atlassian Jira** (CVE-2025-22167): tale vulnerabilità - di tipo *Path Traversal* - consentirebbe a un attaccante, tramite l'invio di richieste HTTP opportunamente predisposte e sfruttando una non corretta validazione da parte del sistema affetto, di accedere a al contenuto di file sensibili, sovrascrivere configurazioni e/o inserire codice malevolo che può portare all'esecuzione di codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Mattermost** (CVE-2025-58075 e CVE-2025-58073): tali vulnerabilità - entrambe di tipo *Missing Authorization* - potrebbero consentire a un utente malintenzionato il bypass dei meccanismi di sicurezza nella gestione degli utenti dei team, manipolando l'*OAuth State* o il *RelayState* sulle istanze target. Ulteriori dettagli nell'alert sul sito dello

CSIRT Italia.

- **Veeam Backup & Replication** (CVE-2025-48984 e CVE-2025-48983): tali vulnerabilità - entrambe di tipo *Remote Code Execution* - permetterebbero a un attaccante - autenticato come un utente di dominio - di eseguire codice arbitrario da remoto tramite l'invio di richieste opportunamente predisposte al servizio di *Mount* (che effettua una corretta validazione dei comandi), compromettendo potenzialmente l'intera infrastruttura di backup qualora questa sia *domain-joined*. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **DNN** (CVE-2025-64095): tale vulnerabilità - di tipo *Unrestricted File Upload* - permetterebbe a un attaccante remoto non autenticato di caricare file arbitrari e sovrascrivere file esistenti sul server a causa della mancanza di controlli di autenticazione e validazione nella funzionalità di upload dell'editor HTML. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **IBM Maximo** (CVE-2025-36386): tale vulnerabilità - di tipo *Authentication Bypass* - permetterebbe a un eventuale attaccante remoto di bypassare i meccanismi di autenticazione e ottenere accesso non autorizzato all'applicazione.
- **DNN** (CVE-2025-59545): tale vulnerabilità - di tipo *Cross-site Scripting (XSS)* - permetterebbe, tramite il modulo *Prompt*, l'esecuzione di comandi che possono restituire HTML grezzo. In tal modo, un input malevolo, anche se sanificato per la visualizzazione in altri contesti, potrebbe essere eseguito quando viene elaborato tramite determinati comandi, portand o a una potenziale esecuzione di script (XSS).
- **Redis** (CVE-2025-49844): tale vulnerabilità - di tipo *Use-After-Free* - e riguardante la componente di scripting Lua, potrebbe consentire a utenti malintenzionati di eseguire da remoto codice arbitrario tramite uno script Lua appositamente predisposto. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Adobe Commerce/Magento** (CVE-2025-54236): tale vulnerabilità - di tipo *Improper Input Validation* - potrebbe permettere a un attaccante non autenticato di manipolare sessioni e oggetti applicativi, con possibili conseguenze quali l'impersonificazione di account utente, takeover di sessione e, su sistemi che preservano la sessione all'interno di file, possibile esecuzione remota di codice. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Netbird** (CVE-2025-10678): durante l'installazione (del prodotto tramite lo script fornito dal vendor, viene creato automaticamente un account amministrativo per la componente ZITADEL (identity provider integrato). Tuttavia, lo script non rimuove né modifica la password di default utilizzata per l'account. Un attaccante potrebbe sfruttare tali credenziali predefinite per ottenere accesso non autorizzato all'applicazione. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **FlowiseAI** (CVE-2025-61913): tale vulnerabilità - di tipo *Path Traversal* - permetterebbe a un eventuale attaccante autenticato di leggere e scrivere file arbitrari in qualsiasi percorso del file system ed eseguire potenzialmente da remoto codice arbitrario sui sistemi affetti, sfruttando i componenti *WriteFileTool* e *ReadFileTool* di Flowise, i quali non limitano correttamente l'accesso ai percorsi dei file. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Veeder-Root TLS4B** (CVE-2025-58428): tale vulnerabilità - *Command Injection* - consentirebbe a un eventuale attaccante di ottenere accesso completo alla shell, eseguire comandi da remoto, muoversi lateralmente all'interno della rete, provocare condizioni di *Denial of Service*, causare il blocco dell'accesso amministrativo e compromettere le funzionalità principali del sistema.
- **Gladinet CentreStack e TrioFox** (CVE-2025-11371): tale vulnerabilità - di tipo *Local File Inclusion* - se sfruttata in combinazione con la CVE-2025-30406 potrebbe consentire a un attaccante non autenticato di accedere a file di sistema ed eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Fortinet FortiSwitchManager** (CVE-2025-49201): tale vulnerabilità - di tipo *Weak Authentication* - relativa alla componente WAD/GUI, consentirebbe ad un attaccante di bypassare l'autenticazione attraverso attacchi di tipo

- brute-force. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle E-Business Suite** (CVE-2025-61884): tale vulnerabilità – di tipo *Unauthorized Access* – consentirebbe a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte e la non corretta validazione delle stesse, di accedere a dati sensibili e compromettere parzialmente i sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Oracle E-Business Suite** (CVE-2025-62481 e CVE-2025-53072): tali vulnerabilità – entrambe di tipo *Missing Authentication for Critical Function* – consentirebbero a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte e la non corretta validazione delle stesse da parte del componente "Marketing", di eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **VMware Aria Operations** (CVE-2025-41244): tale vulnerabilità – di tipo zero-day e *Local Privilege Escalation* – qualora sfruttata, potrebbe consentire ad un attaccante con accesso non amministrativo a una macchina virtuale gestita da Aria Operations – con il *Software Development Management Pack (SDMP)* abilitato e VMware tools installati – di elevare i propri privilegi sul sistema impattato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
  - **Ivanti Endpoint Manager** (CVE-2025-9713 e CVE-2025-11622): tali vulnerabilità – di tipo rispettivamente *Path Traversal* e *Deserialization of Untrusted Data* – consentirebbero, senza necessità di autenticazione e tramite interazione utente, l'esecuzione di codice da remoto (relativo alla CVE-2025-9713, presente nel metodo "OnSaveToDB") e a un attaccante autenticato localmente di elevare i propri privilegi (relativo alla CVE-2025-11622, presente nel servizio "AgentPortal"). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

## Novembre

- **WatchGuard Firebox** (CVE-2025-59396): tale misconfigurazione – associata originariamente alla vulnerabilità CVE-2025-59396 rifiutata dal vendor – permetterebbe a un eventuale attaccante di ottenere un accesso amministrativo tramite un'interfaccia amministrativa esposta tramite protocollo SSH sulla porta 4118 utilizzando le credenziali predefinite, laddove esse non siano state esplicitamente sostituite in fase di installazione dei dispositivi.
- **SolarWinds Web Help Desk** (CVE-2025-40549, CVE-2025-40548 e CVE-2025-40547): tali vulnerabilità – rispettivamente di tipo *Code Injection*, *Improper Privilege Management* e *Path Traversal* – potrebbero consentire a un utente malintenzionato con privilegi di amministratore di eseguire codice arbitrario sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Django** (CVE-2025-64459): tale vulnerabilità – di tipo *SQL Injection* – potrebbe consentire a un attaccante remoto non autenticato di inviare un input malevolo, interpretato direttamente dal motore SQL, portando potenzialmente all'accesso non autorizzato ai dati, alla modifica e/o cancellazione di informazioni e all'esecuzione di comandi arbitrari sul database relativo al backend dell'applicazione web. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Open Source Geospatial Foundation GeoServer** (CVE-2025-58360): tale vulnerabilità – di tipo *XML External Entity Reference (XXE)* – permetterebbe a un eventuale attaccante di generare entità esterne arbitrarie sui sistemi target e di accedere potenzialmente a file o servizi interni, comportando così l'accesso a informazioni sensibili o provocare altro genere di impatti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Grafana Enterprise** (CVE-2025-41115): tale vulnerabilità – di tipo *Incorrect Privilege Assignment* – permetterebbe a un eventuale attaccante di elevare i propri privilegi o di impersonificare altri utenti sui sistemi interessati, qualora il prodotto sia configurato con la funzionalità di "SCIM provisioning" attiva e sia abilitata la sincronizzazione automatica

degli utenti sulla base delle richieste inviate tramite tale protocollo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **SuiteCRM** (CVE-2025-64493 e CVE-2025-64492): tali vulnerabilità – di tipo *SQL Injection* – permetterebbero a un eventuale attaccante autenticato di sfruttare una SQL injection di tipo "blind" e "time-based" per estrarre dati arbitrari - anche potenzialmente sensibili, nel caso della CVE-2025-64492 - dal database senza alcun privilegio amministrativo e compromettendone così la confidenzialità.
- **Fortinet FortiWeb** (CVE-2025-58034): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante autenticato di eseguire comandi arbitrari sul sistema operativo sottostante tramite richieste HTTP appositamente predisposte veicolate tramite API o specifici comandi CLI. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **PostgreSQL pgAdmin** (CVE-2025-12762): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante di iniettare ed eseguire comandi arbitrari da remoto sul server che ospita pgAdmin. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **W3 Total Cache** (CVE-2025-9501): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante di eseguire codice PHP arbitrario mediante l'inserimento di payload malevoli in commenti o input elaborati dal plugin. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Open WebUI** (CVE-2025-64495): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe a un eventuale attaccante autenticato e con i permessi per creare prompt, di inserire un payload malevolo che potrebbe essere eseguito da altri utenti se questi utilizzano il comando con l'opzione "Insert Prompt as Rich Text" attiva. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Symfony** (CVE-2025-64500): tale vulnerabilità – di tipo *Incorrect Authorization* – permetterebbe a un eventuale attaccante di accedere a risorse protette bypassando i controlli di accesso tramite manipolazione del percorso dell'URL. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **OpenWRT** (CVE-2025-62526 e CVE-2025-62525): tali vulnerabilità – rispettivamente di tipo *Out-of-bounds Read/Write* e *Buffer Overflow* – permetterebbero a un eventuale attaccante nella rete locale dei sistemi affetti rispettivamente di leggere/scrivere aree di memoria riservate al Kernel con la possibilità di effettuare *sandbox escape* (CVE-2025-62525) ed eseguire codice arbitrario, sfruttando una falla nel codice utilizzato per il parsing degli eventi di registrazione alla rete (CVE-2025-62526). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Monsta FTP** (CVE-2025-34299): tale vulnerabilità – di tipo *Unrestricted File Upload* – permetterebbe a un eventuale attaccante, tramite un file opportunamente predisposto su un server FTP da lui controllato, di scaricare tale file in un percorso arbitrario sui sistemi affetti e portando potenzialmente all'esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Twonky Server** (CVE-2025-13316 e CVE-2025-13315): tali vulnerabilità – di tipo *Authentication Bypass* – permetterebbero a un eventuale attaccante di ottenere le credenziali dell'utente amministratore, eludendo i meccanismi di autenticazione sui sistemi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Asus AiCloud** (CVE-2025-59366): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante di eseguire alcuni comandi senza autorizzazione sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **R.V.R Elettronica TEX** (CVE-2025-63207): tale vulnerabilità – di tipo *Improper Authentication* – permetterebbe a un eventuale attaccante di modificare le credenziali degli account "Admin", "Operator" e "User" attraverso richieste POST non autenticate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache OFBiz** (CVE-2025-61623, CVE-2025-59118): tali vulnerabilità – di tipo *Unrestricted File Upload* e *Cross-site*

*Scripting (XSS)* – permetterebbero, rispettivamente, a un eventuale attaccante remoto di caricare file malevoli sul target e di eseguire codice arbitrario lato client. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

- **N-Able N-Central** (CVE-2025-11700): tale vulnerabilità – di tipo *XML External Entity Reference (XXE)* – permetterebbe a un eventuale attaccante, sfruttando entità XML esterne, di leggere file sensibili dal file system del server ed esfiltrare informazioni riservate, inducendo l’applicazione a restituire come output il contenuto dei file. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **MLflow** (CVE-2025-11200): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante remoto di bypassare i meccanismi di autenticazione e ottenere accesso non autorizzato all’applicazione e i suoi modelli, nonché di creare credenziali estremamente deboli o vuote.

## Dicembre

- **WatchGuard Firewall OS** (CVE-2025-14733): tale vulnerabilità – di tipo *Out-of-bounds Write* – permetterebbe a un attaccante non autenticato di eseguire codice arbitrario da remoto sulle istanze impattate, sfruttando una gestione non corretta della lunghezza dei payload IKEv2 da parte del componente iked. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Moodle** (CVE-2025-67847, CVE-2025-67848, CVE-2025-67849, CVE-2025-67850, CVE-2025-67855): tali vulnerabilità – rispettivamente di tipo Remote Code Execution, Authentication Bypass, Cross Site Scripting (XSS) e Reflected Cross Site Scripting (Reflected XSS) – potrebbero consentire a un attaccante remoto di eseguire codice arbitrario da remoto, eludere i meccanismi di autenticazione, sottrarre sessioni attive e impartire comandi lato client. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Fortinet FortiSwitchManager, FortiProxy, FortiOS e FortiWeb** (CVE-2025-59718, CVE-2025-59719): tali vulnerabilità – di tipo *Improper Access Control* – permetterebbero a un eventuale attaccante non autenticato di eludere i meccanismi di autenticazione tramite l’invio di una risposta SAML (Security Assertion Markup Language) opportunamente predisposta. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **SonicWall SMA1000** (CVE-2025-40602): tale vulnerabilità – di tipo *Missing Authorization* – qualora sfruttata insieme alla CVE-2025-23006 – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un eventuale attaccante non autenticato di ottenere accesso con account non privilegiato sulle istanze interessate e successivamente sfruttando la prima, elevare i privilegi fino a root, ottenendo il controllo delle istanze impattate. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Meta React e Vercel Next.js** (CVE-2025-55182): tale vulnerabilità – di tipo *Insecure Deserialization* – permetterebbe a un eventuale attaccante di eseguire codice da remoto sulle istanze interessate. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **MongoDB** (CVE-2025-14847): tale vulnerabilità – di tipo *Improper Handling of Length Parameter Inconsistency* – permetterebbe a un eventuale attaccante non autenticato l’accesso da remoto non controllato a zone di memoria riservate e, potenzialmente, accedere a informazioni sensibili. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Mattermost** (CVE-2025-12419, CVE-2025-12421): tali vulnerabilità – di tipo *Weak Authentication* – potrebbero consentire a un utente malintenzionato il bypass dei meccanismi di sicurezza e il takeover degli account dei team sulle istanze target. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Microsoft Kestrel** (CVE-2025-55315): tale vulnerabilità – di tipo *HTTP Request/Response Smuggling* – e relativa a ASP.NET Core permetterebbe a un eventuale attaccante remoto di effettuare il bypass di meccanismi di sicurezza.

Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **NopSolutions nopCommerce** (CVE-2025-11699): tale vulnerabilità – di tipo *Insufficient Session Expiration* – permetterebbe a un eventuale attaccante in possesso dei cookie di sessione di un utente autenticato di impersonare tale utente sul sistema interessato anche nel caso che quest'ultimo abbia già effettuato log out.
- **Gogs** (CVE-2025-8110): tale vulnerabilità – di tipo *Path Traversal* – dovuta ad una non corretta gestione dei link simbolici da parte della API *PutContents* potrebbe consentire a un attaccante autenticato con permessi minimi, di creare simlink che puntano a percorsi esterni all'area controllata da Gogs, rendendo possibile la scrittura di file al di fuori del repository e l'esecuzione di codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Traccar** (CVE-2025-61666): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante di non autenticato di accedere a file arbitrari all'interno del file system, inclusi quelli contenenti le password e i file di configurazione dei sistemi affetti.
- **n8n** (CVE-2025-68613): tale vulnerabilità – di tipo *Improper Control of Dynamically-Managed Code Resources* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario con i privilegi del processo n8n. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Gladinet CentreStack e TrioFox** (CVE-2025-14611): tale vulnerabilità – di tipo *Use of Hard-coded Credentials* – permetterebbe a un eventuale attaccante non autenticato di accedere ai file locali, ottenendo informazioni sensibili che potrebbero essere sfruttate per compromettere le istanze interessate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Elastic Kibana** (CVE-2025-59840): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe a un eventuale attaccante di inserire codice malevolo all'interno del Document Object Model (*DOM-Based XSS*) dei sistemi interessati (nel caso abbiano essi le visualizzazioni Vega abilitate, opzione abilitata di default sulle installazioni), che potrebbe poi essere eseguito tramite successive interazioni dell'utente con la risorsa. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Xwiki** (CVE-2025-55749): tale vulnerabilità – di tipo *Improper Access Control* – permetterebbe a un eventuale attaccante di leggere qualsiasi file all'interno della cartella *webapp* di XWiki, potenzialmente contenenti credenziali. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **ConnectWise ScreenConnect** (CVE-2025-14265): tale vulnerabilità – di tipo *Download of Code Without Integrity Check* – permetterebbe a un eventuale attaccante di accedere a dati di configurazione o l'installazione e l'esecuzione di codice arbitrario, sotto forma di estensioni non sicure, da parte dei sistemi affetti.
- **Cisco Secure Email e Web Manager** (CVE-2025-20393): tale vulnerabilità – di tipo *Improper Input Validation* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.



**Agenzia per la  
Cybersicurezza Nazionale**



---

**OPERATIONAL SUMMARY**  
**Il semestre 2025**