



Agenzia per la
Cybersicurezza Nazionale



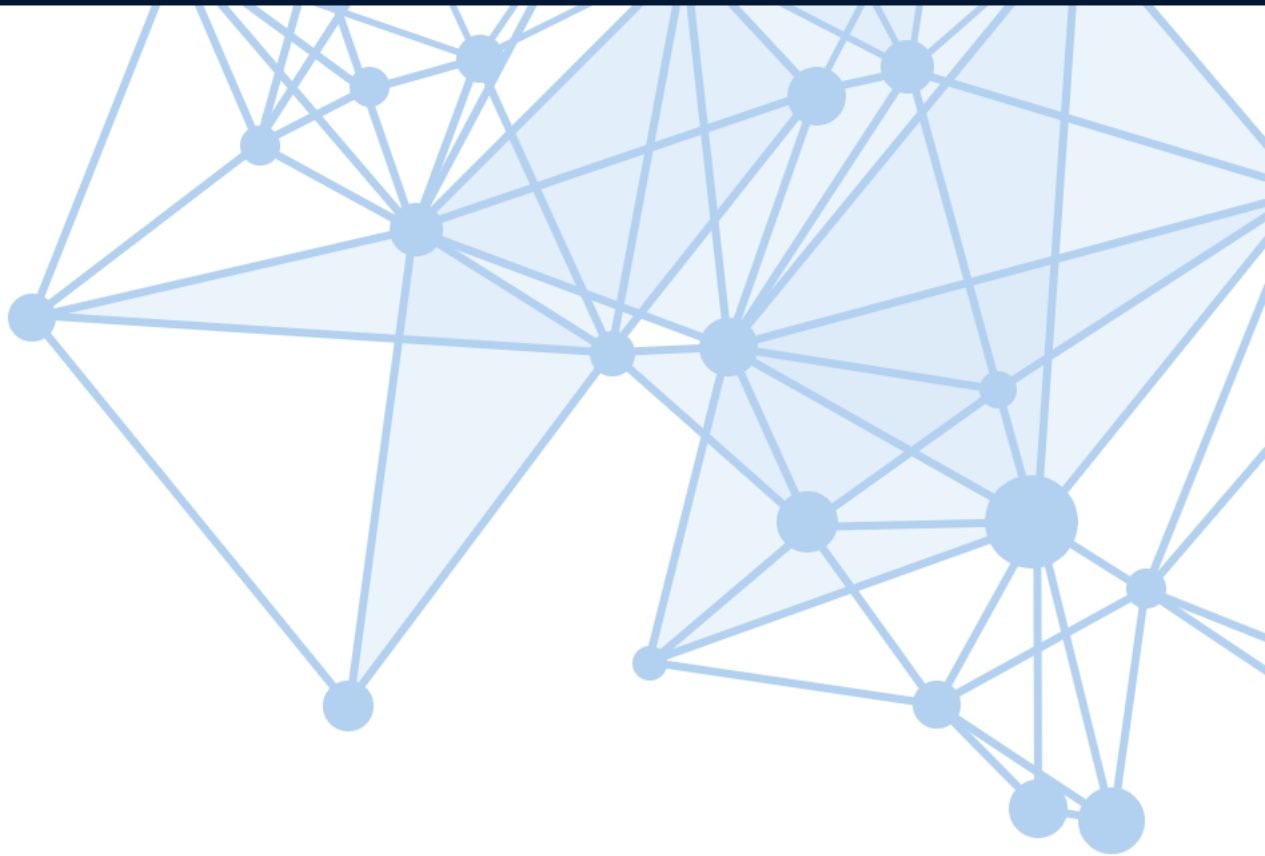
OPERATIONAL SUMMARY

GENNAIO 2026

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni
e gestione delle crisi cyber

TLP:CLEAR



INTRODUZIONE

Il presente documento riporta su base mensile alcuni numeri e indicatori derivanti dalle attività operative dell’Agenzia per la Cybersicurezza Nazionale, utili per caratterizzare lo stato della minaccia cyber in Italia. In particolare, il CSIRT Italia, articolazione tecnico-operativa dell’Agenzia, è hub nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di Sicurezza Nazionale Cibernetica, Legge 28 giugno 2024, n. 90, Direttiva NIS) e riceve altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni dotano l’Agenzia 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 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 di 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](#).



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

1. EXECUTIVE SUMMARY	5
2. EVENTI ED INCIDENTI	9
2.1. Settori impattati	10
2.2. Tipologia di minacce negli eventi	11
2.3. Distribuzione delle minacce per settore	12
2.4. Distribuzione geografica delle vittime	13
3. VULNERABILITÀ	14
3.1. Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia	14
3.2. Distribuzione delle vulnerabilità sui vendor	15
3.3. CWE nel mese	16
3.4. Vulnerabilità con maggior probabilità di sfruttamento	17
4. MINACCIA	19
4.1. Ransomware: distribuzione delle vittime	19
4.2. Rivendicazioni ransomware	20
4.3. Rivendicazioni DDoS	21
5. MONITORAGGIO	22
5.1. Comunicazioni dirette	22

Elenco delle figure

Figura 1 - indicatori delle attività operative a gennaio 2026 e nei sei mesi precedenti	7
Figura 2 - andamento attività reattive e analisi previsionale	9
Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente (top 15)	10
Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al semestre precedente (top 15)	11
Figura 5 - numero di vittime per settore e tipologia di minacce	12
Figura 6 - distribuzione delle vittime degli eventi cyber	13
Figura 7 - top 25 produttori affetti da vulnerabilità nel mese	15
Figura 8 - top 25 prodotti affetti da vulnerabilità nel mese	16
Figura 9 - top 5 CWE nel mese	16
Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità	19
Figura 11 - andamento delle rivendicazioni Ransomware	20
Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni	20
Figura 13 - andamento delle rivendicazioni DDoS	21
Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni	21
Figura 15 - distribuzione delle segnalazioni per tipologia di soggetto	24

1

EXECUTIVE SUMMARY

▪ Eventi e Incidenti

Nel mese di gennaio 2026 sono stati registrati **225 eventi**, in **aumento** del 42% rispetto ai **158** di dicembre, mentre il numero di **incidenti (39)** è in **diminuzione** del 13% rispetto al mese precedente. La crescita generalizzata degli eventi è riconducibile, da una parte, alla naturale oscillazione dei fenomeni monitorati, dall'altra, all'**incremento di circa il 75% delle notifiche ricevute dal CSIRT Italia**. Ciò in esito all'entrata in vigore, nel corso del gennaio 2026, dei nuovi obblighi previsti dal Decreto legislativo n. 138/2024.

Nel mese di gennaio, il **brand abuse** ha rappresentato la principale tipologia di minaccia rilevata. Tale fenomeno comprende un insieme di pratiche malevole volte a sfruttare il valore, la notorietà e la reputazione di marchi riconosciuti per finalità fraudolente. In stretta correlazione con il brand abuse, il **phishing** si è confermato nel mese di gennaio come la seconda minaccia più rilevante. Contestualmente, è stato rilevato un aumento delle attività di **scansione attiva su credenziali**, riconducibili a operazioni automatizzate finalizzate all'identificazione di password deboli, impropriamente configurate o esposte su sistemi informatici.

▪ Settori interessati

I settori con il maggior numero eventi cyber registrati nel mese sono stati: **Manifatturiero, Tecnologico e Sanitario**. Il primo è stato principalmente interessato da ransomware e compromissioni di caselle e-mail. Il settore tecnologico da malware e intrusioni, i soggetti nel settore sanitario da ransomware ed esposizioni di dati (ulteriori dettagli in sezione 2.3).

▪ Ransomware

Gli attacchi ransomware hanno interessato prevalentemente i settori manifatturiero, tecnologico e sanitario, che risultano essere i più colpiti nel mese di gennaio. L'analisi degli eventi rilevati evidenzia come i principali vettori di compromissione siano riconducibili all'utilizzo di credenziali valide, precedentemente compromesse, e allo sfruttamento di servizi di accesso remoto non adeguatamente configurati.

▪ Attacchi DDoS

Nel mese di gennaio, gli eventi riconducibili a fenomeni di **hacktivism** hanno rappresentato circa il 4% del totale degli eventi rilevati, in ulteriore diminuzione rispetto al mese di dicembre, nel quale si attestavano intorno al 10%. Tale flessione si inserisce in una dinamica

di natura ciclica che caratterizza questo ambito di minaccia, con alternanza di fasi di ridotta intensità e periodi di maggiore attivismo, accompagnati da un incremento delle rivendicazioni online.

▪ Monitoraggio proattivo

Nell'ambito dell'attività proattiva di monitoraggio della superficie esposta dei soggetti nazionali, il CSIRT Italia ha inviato, a gennaio 2026, **1.010 comunicazioni di allertamento** a pubbliche amministrazioni e imprese appartenenti alla constituency, relative all'esposizione su Internet di **1.409** servizi a rischio.

L'analisi dei *log* provenienti da **malware di tipo infostealer** ha consentito, infine, di identificare **17 account** potenzialmente compromessi, afferenti a soggetti istituzionali, tutti prontamente allertati.

▪ Vettori di attacco

I punti di ingresso più frequenti a gennaio 2026 sono stati le e-mail, l'utilizzo di account validi e lo sfruttamento di vulnerabilità di note.

▪ Vulnerabilità

Sono state pubblicate **5.144** nuove CVE, in **diminuzione (-491)** rispetto a dicembre. Di queste, **731** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione (-24)**, e per **7** CVE è stato rilevato lo sfruttamento attivo, in **diminuzione (-7)** rispetto a dicembre. Di rilievo, in ragione del loro elevato livello di criticità,

le vulnerabilità relative ai prodotti **Oracle** HTTP Server e Oracle WebLogic Server Proxy Plug-in (CVE-2026-21962), nonché a FortiOS, FortiProxy e FortiSwitchManager di **Fortinet** (CVE-2025-59718), caratterizzate da potenziali impatti rilevanti sulla riservatezza, integrità e disponibilità dei sistemi informativi. Tali criticità potrebbero consentire, in specifici scenari, l'accesso non autorizzato a risorse e dati sensibili, nonché l'acquisizione indebita di privilegi amministrativi mediante l'elusione dei meccanismi di autenticazione, esponendo così i sistemi interessati a elevati rischi di compromissione. Sono state pertanto oggetto di specifiche attività di allertamento condotte da parte del CSIRT Italia. Le vulnerabilità individuate hanno inoltre determinato un incremento del numero di sistemi e servizi potenzialmente esposti, con conseguente aumento delle comunicazioni di allertamento effettuate dall'Agenzia ai sensi dell'art. 2, comma 1, della Legge n. 90/2024, finalizzate a favorire l'adozione tempestiva degli interventi risolutivi da parte dei soggetti interessati.

▪ Allertamento

Le **comunicazioni dirette**, effettuate dal CSIRT Italia per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane, nel mese di gennaio 2026 sono state in totale **3.909**, in sensibile **aumento** rispetto a dicembre.

I NUMERI DI GENNAIO 2026

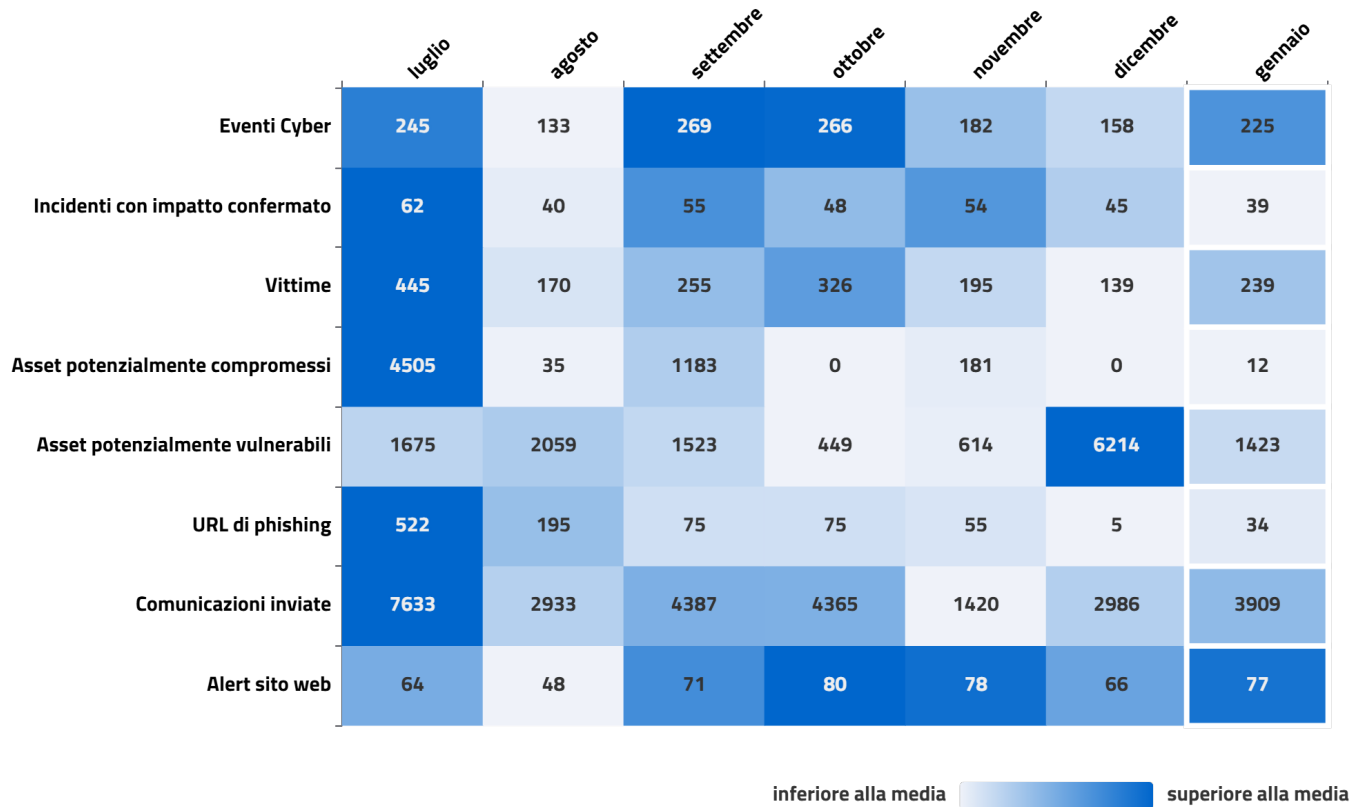


Figura 1 - indicatori delle attività operative a gennaio 2026 e nei sei mesi precedenti

- **225** eventi cyber, in **aumento (+67)**;
- **239** vittime, in **aumento (+99)**;
- **153** vittime della constituency¹, in **aumento (+108)**;
- **39** incidenti con impatto confermato, in **diminuzione (-6)**;
- **12** asset potenzialmente compromessi, in **aumento (+12)**;
- **1.423** asset potenzialmente vulnerabili, in **diminuzione (-4.791)**;
- **77** alert sul sito web del CSIRT Italia, in **aumento (+11)**;
- **3.909** comunicazioni inviate, in **aumento (+923)**;
- **5.144** nuove CVE, in **diminuzione (-491)**.

¹La 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 **l'elenco dei prodotti** che a gennaio 2026 sono stati oggetto di specifici alert pubblicati sul sito web del CSIRT Italia a causa di vulnerabilità. Tali vulnerabilità, oggetto di alert o perché di recente scoperta oppure perché ne è stato rilevato lo sfruttamento, **richiedono l'adozione tempestiva di aggiornamenti di sicurezza** o delle misure di mitigazione disponibili nell'alert di seguito referenziato.

- **GNU telnetd** (CVE-2026-24061) Link all'alert;
- **Trend Micro** (CVE-2025-69260, CVE-2025-69259, CVE-2025-69258) Link all'alert;
- **Fortinet FortiManager, FortiOS, FortiProxy, FortiAnalyzer e FortiWeb** (CVE-2026-24858) Link all'alert;
- **Fortinet FortiSwitchManager, FortiOS e FortiSIEM** (CVE-2025-25249, CVE-2025-64155) Link all'alert;
- **ZimbraCollaborationSuite** (CVE-2025-68645) Link all'alert;
- **SmarterTools SmarterMail** (CVE-2025-52691) Link all'alert, (CVE-2026-23760) Link all'alert;
- **N8n** (CVE-2026-21877, CVE-2025-68668, CVE-2026-21858, CVE-2026-0863, CVE-2026-1470) Link all'alert;
- **Oracle Corporation Oracle HTTP Server e Oracle Weblogic Server Proxy Plug-in** (CVE-2026-21962) Link all'alert;
- **Ivanti Endpoint Manager Mobile** (CVE-2026-1340, CVE-2026-1281) Link all'alert;
- **Veeam Backup and Recovery** (CVE-2025-59470, CVE-2025-59469, CVE-2025-55125) Link all'alert;
- **Craftcms cms** (CVE-2025-68455, CVE-2025-68437, CVE-2025-68454) Link all'alert;
- **Coollabsio coolify** (CVE-2025-64419, CVE-2025-64420, CVE-2025-64424) Link all'alert;
- **Cisco Unified Communications Manager, Unified Communications Manager IM and Presence Service e Unity Connection** (CVE-2026-20045) Link all'alert;
- **Calcom cal.com** (CVE-2026-23478) Link all'alert.

Maggiori dettagli nelle sezioni 3 e 5.

2

EVENTI ED INCIDENTI

A gennaio 2026 sono stati individuati **225** eventi cyber, in **aumento** del 42% rispetto al mese precedente. Questi ultimi hanno **interessato 194 soggetti nazionali**: 153 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 225 eventi cyber, **39 sono stati classificati quali incidenti**, in **diminuzione** del 13% rispetto a dicembre.

La Figura 2 mostra l'andamento di eventi e incidenti fino al mese in esame, corredato da una previsione, basata sull'analisi dei dati precedenti², riferita ai successivi 3 mesi.

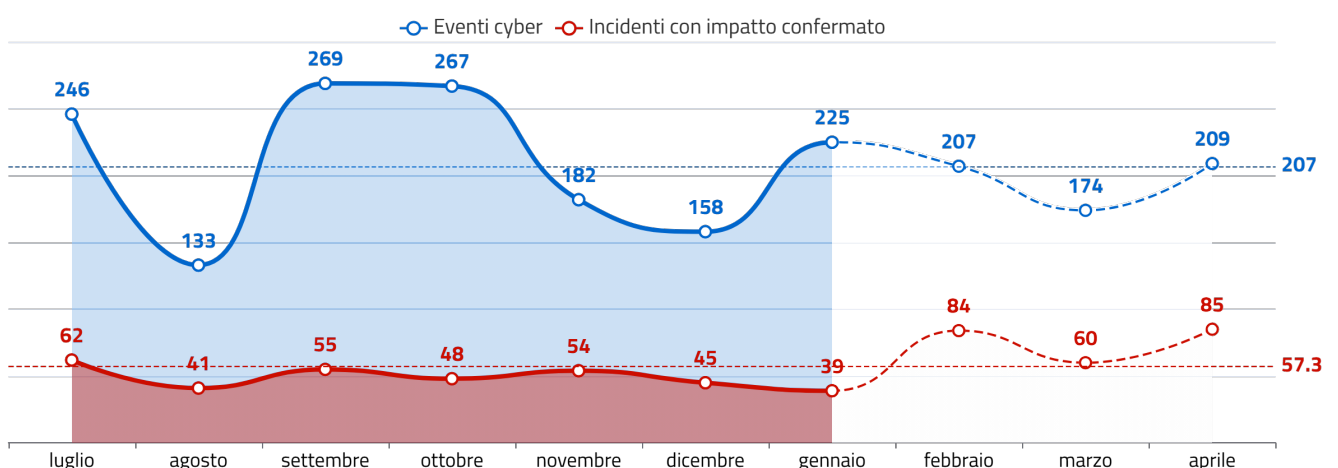


Figura 2 - andamento attività reattive e analisi previsionale

² La previsione dà un'idea generale degli andamenti futuri utilizzando un modello ARIMA (AutoRegressive Integrated Moving Average). È importante sottolineare che la previsione non può essere accurata in quanto il manifestarsi degli eventi dipende da molti fattori, tra i quali quelli di natura geopolitica, la scoperta di nuove vulnerabilità, la capacità degli attaccanti e così via.

2.1 Settori impattati

In figura 3 si riporta il numero di vittime di eventi per settore impattato³. Si evidenzia altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico).

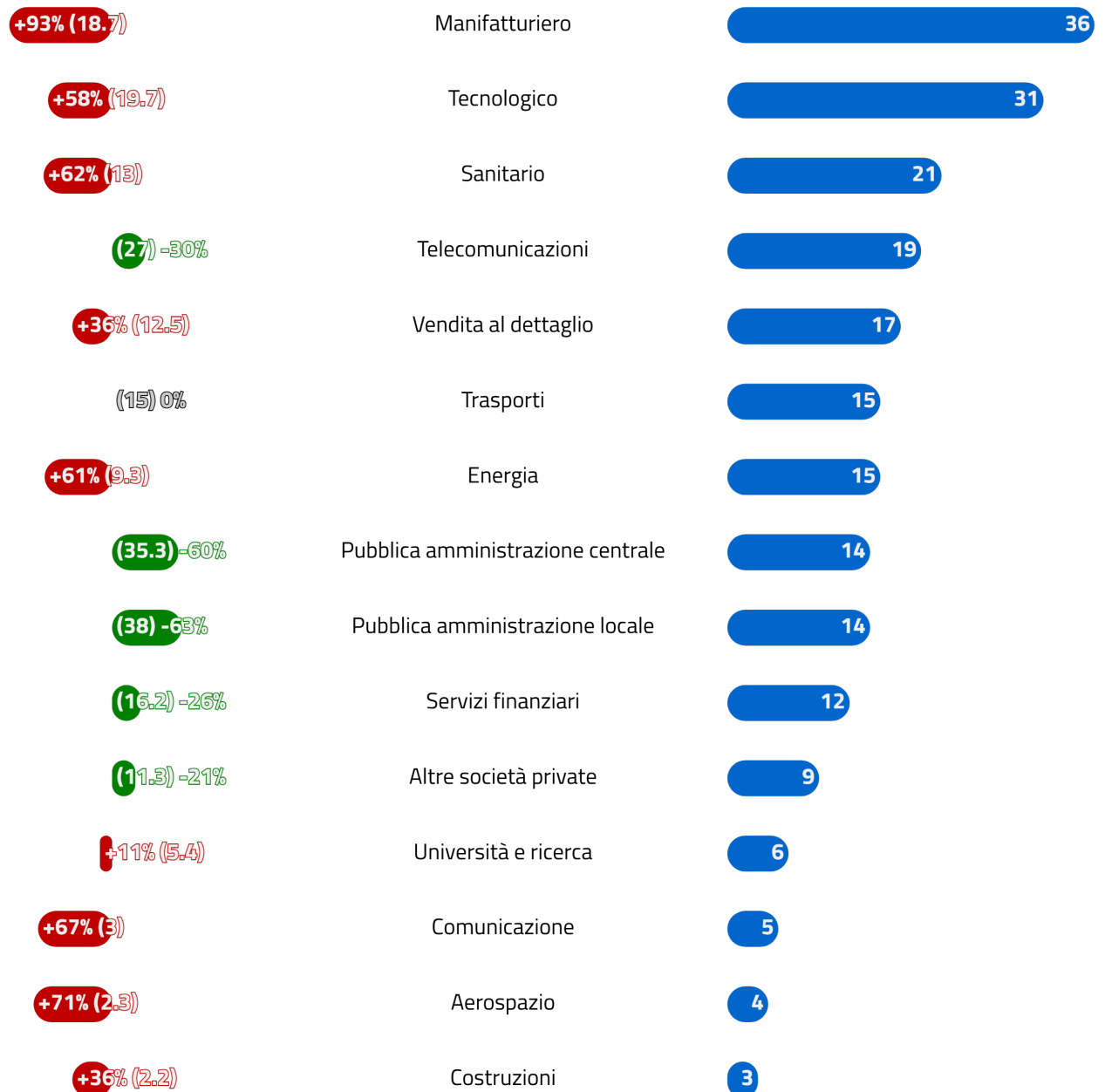


Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente (top 15)

³ 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 eventi⁴ e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).

Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (<https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn>).

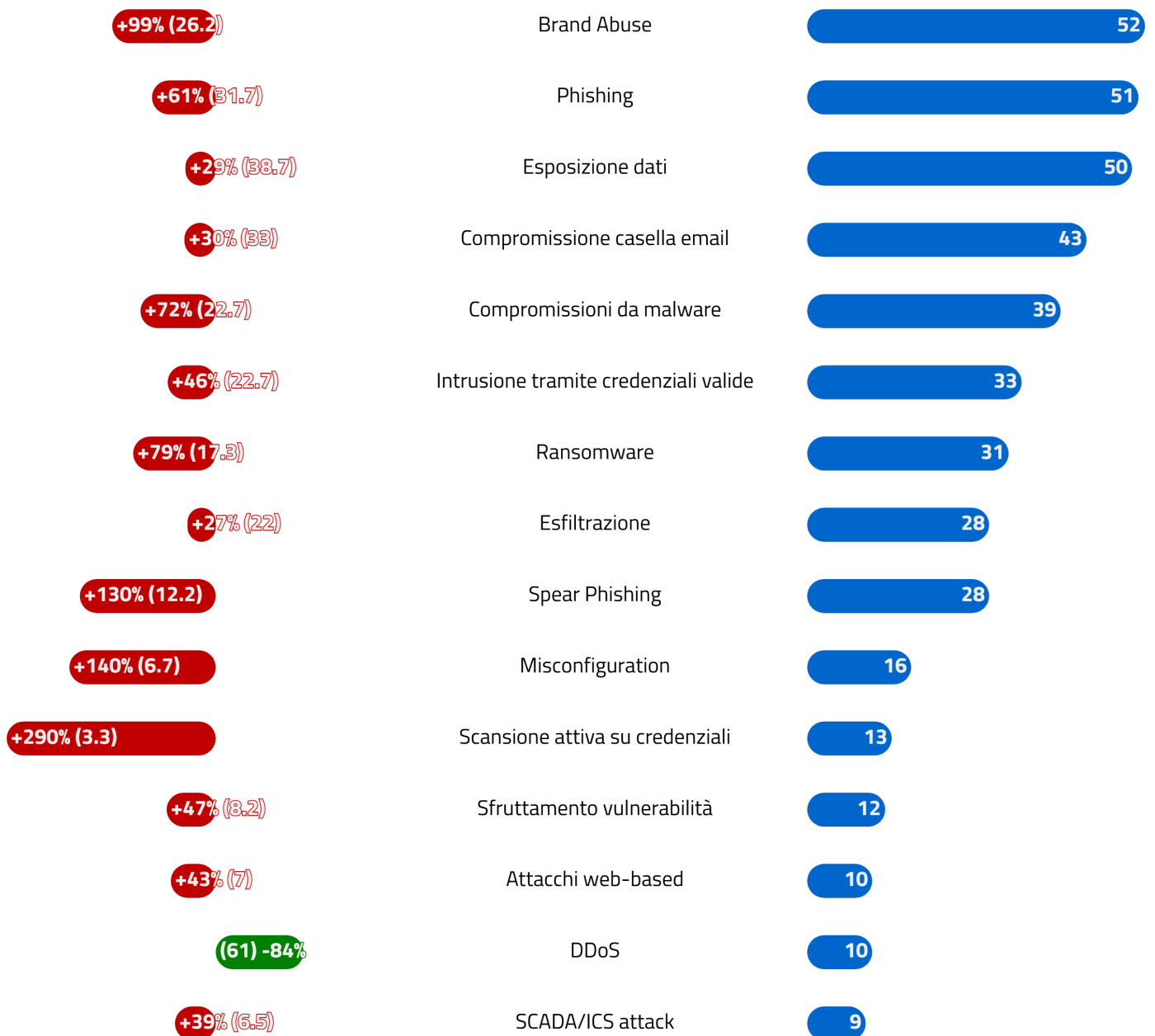


Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al semestre precedente (top 15)

⁴ 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, ottenuto analizzando gli eventi di gennaio 2026. 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>). In Figura sono mostrati solo i 15 settori più interessati dalle minacce.

	Manfatturiero	Tecnologico	Vendita al dettaglio	Sanitario	Pubblica amministrazione centrale	Energia	Pubblica amministrazione locale	Servizi finanziari	Trasporti	Telecomunicazioni	Altre società private	Università e ricerca	Aerospazio	Assicurazioni	Costruzioni
Compromissioni da malware	10	8	7	6	1	2	3		4	3	2		1		
Esposizione dati	8	5	6	4	3	8	1	2	3	2	1		3		1
Brand Abuse	11	3	2	3	4	3	4	6	1	1		2		2	1
Compromissione casella email	10	5	2	2	6	1	2	2	1	4	1	2			1
Phishing	7	5	4	3	3	2	4	6	2		1	1			
Ransomware	13	6	5	5		2	1		4		1			1	
Intrusione tramite credenziali valide	6	7	4	3	2	3	2	1	2	3		1			1
Spear Phishing	7	2		4	4	2	1	3	1		1	3		2	1
Esfiltrazione	6	2	3	1		2	1	1	4	1	2	1	3		
Misconfiguration	4	4		4	3	1	2		2	2					
Scansione attiva su credenziali	1	2	2	4	1	2	1								
Sfruttamento vulnerabilità		2	3	2			1			2	2				
Attacchi web-based		1	2		1	1				2	2				1
DDoS		3		1	2		3			1					
SCADA/ICS attack	2					1	1				2				
Smishing	2				1	1		2							
Cybersquatting	2			1								1		1	
Diffusione malware tramite email	2						2	1							
Defacement			1								2				
Typosquatting								1				1		1	
Supply chain attack	1		1												
DoS			1				1								
Spam e scam					1										
Scansioni attive sul perimetro di rete			1												

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

2.4 Distribuzione geografica delle vittime

I 225 eventi cyber hanno interessato **239** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

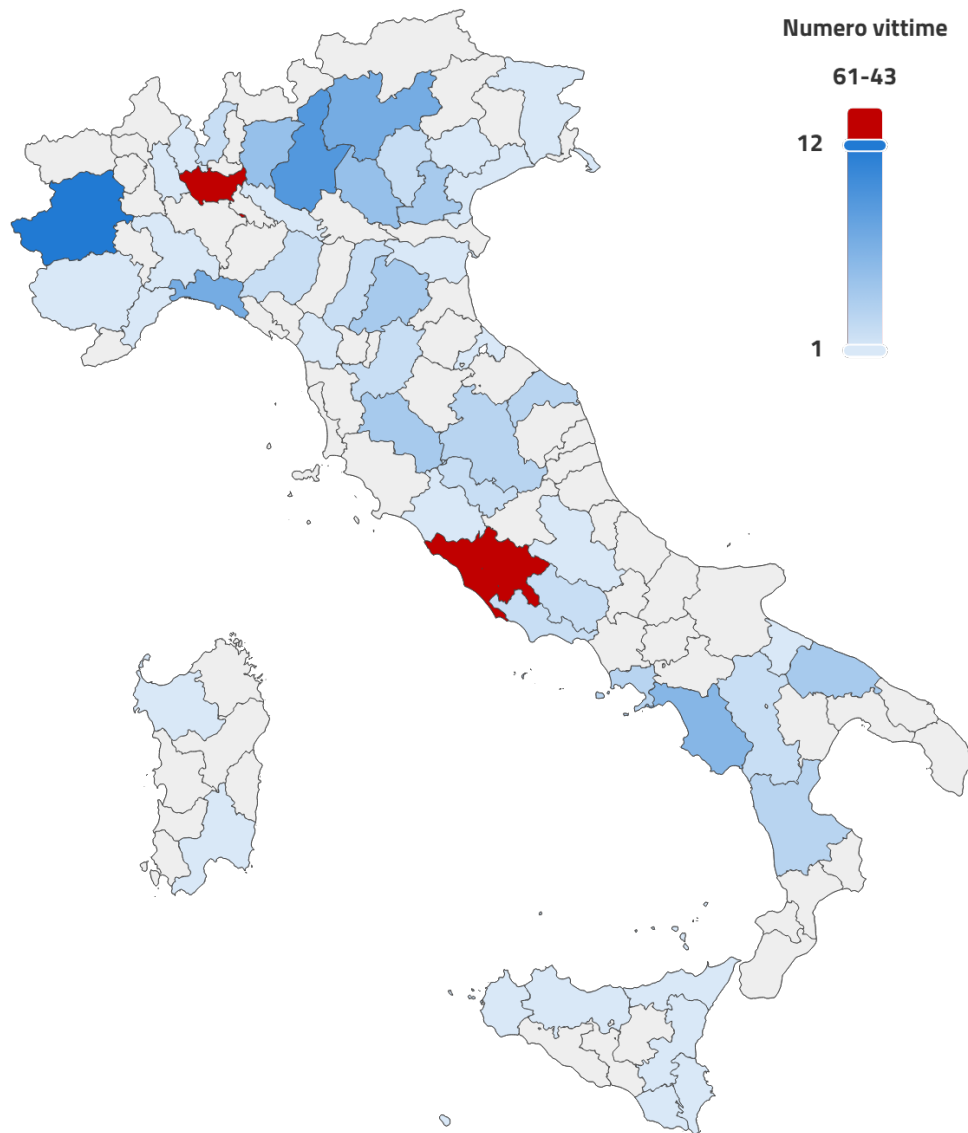


Figura 6 - distribuzione delle vittime degli eventi cyber

3 VULNERABILITÀ

A gennaio 2026 sono state pubblicate⁵ **5.144** nuove CVE, in **diminuzione (-491)** rispetto a dicembre. Di queste, **731** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione (-24)**, e per **7** CVE è stato rilevato lo sfruttamento attivo, in **diminuzione (-7)** rispetto a dicembre.

3.1 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **77**. Oltre al consueto aggiornamento mensile di Microsoft (link) all'alert sul sito web, che ha risolto un totale di 112 nuove vulnerabilità (2 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Fortinet**: fortinet ha recentemente confermato lo sfruttamento attivo in rete di una vulnerabilità di tipo zero-day presente in FortiOS, FortiManager, FortiAnalyzer e FortiProxy. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato, con un account FortiCloud e un dispositivo registrato, di accedere ad altri dispositivi registrati ad account differenti, se l'autenticazione FortiCloud SSO è abilitata su tali dispositivi (stima di impatto sistemico **81,79/100**). Link all'alert del 28/01/2026;
- **n8n**: disponibile un Proof of Concept (PoC) per lo sfruttamento della CVE-2026-21858 – già sanata dal vendor e nota come "Ni8mare" – presente in n8n, piattaforma open source di workflow automation che consente di integrare applicazioni, servizi e API tramite flussi visuali (stima di impatto sistemico **79,48/100**). Link all'alert del 09/01/2026;
- **coolabsio**: disponibili PoC per lo sfruttamento di 3 vulnerabilità con gravità "critica" in Coolify, piattaforma open-source progettata per consentire il deployment e la gestione di applicazioni, database e servizi in modalità self-hosted (stima di impatto sistemico **79,35/100**). Link all'alert del 12/01/2026;
- **GNU telnetd**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2026-24061, di gravità "critica", che interessa il demone telnetd appartenente alla suite di utility di rete GNU Inetutils. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto di aggirare i meccanismi di autenticazione ed ottenere un

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

accesso con privilegi di utente "root" sui sistemi target (stima di impatto sistemico **79,23/100**). Link all'alert del 25/01/2026;

- **Gogs**: rilevato lo sfruttamento attivo in rete della vulnerabilità con gravità "alta" CVE-2025-8110 relativa a Gogs, un popolare servizio Git self-hosted. La vulnerabilità potrebbe consentire ad un utente malintenzionato, autenticato con permessi minimi, di creare un symlink all'interno di un repository che punti a file critici del sistema e di caricare dati attraverso le API che sovrascrivono direttamente questi file. Tale circostanza permetterebbe di eseguire, da remoto, comandi arbitrari sul server (stima di impatto sistemico **76.28/100**). Link all'alert dell'11/12/2025.

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

3.2 Distribuzione delle vulnerabilità sui vendor

In Figura 7 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor⁶.

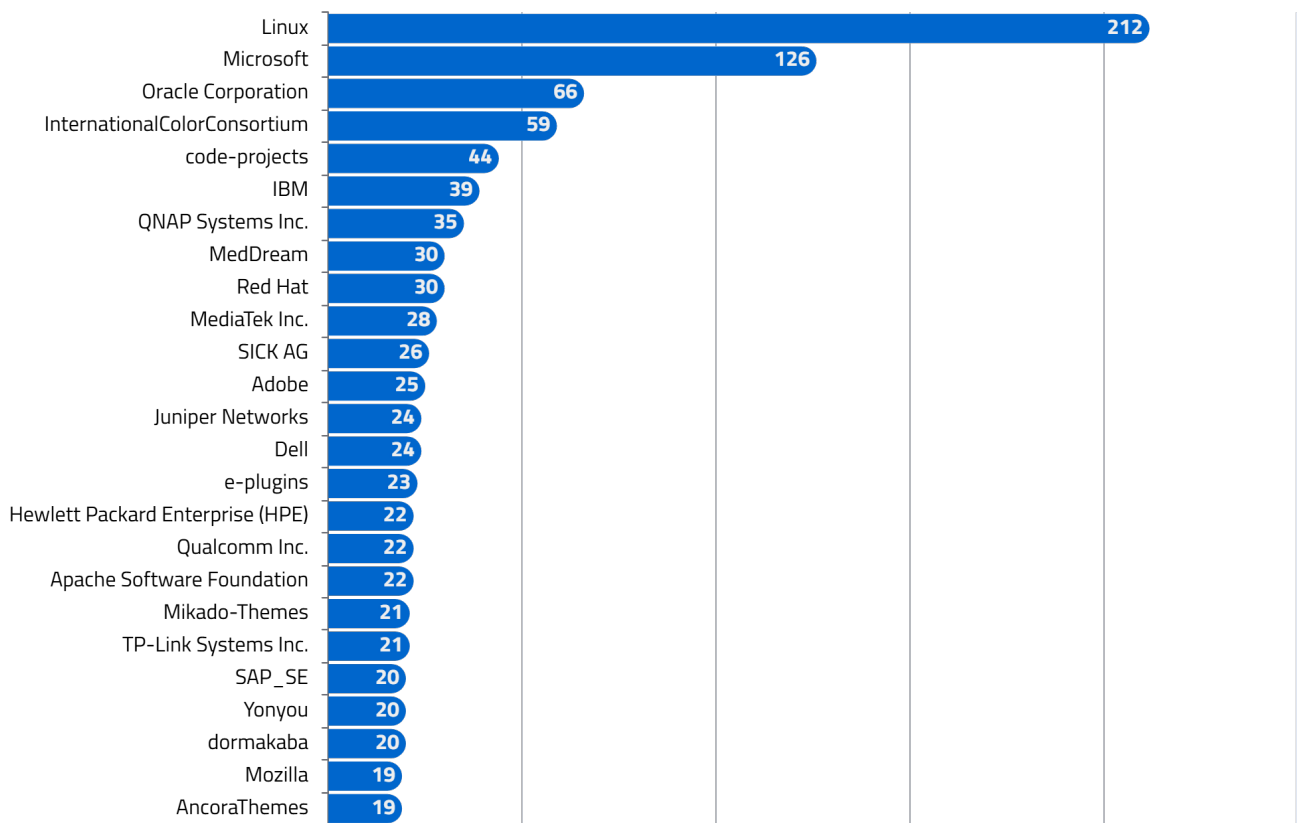


Figura 7 - top 25 produttori affetti da vulnerabilità nel mese

⁶I valori attribuiti alla voce *Linux* si riferiscono esclusivamente alle vulnerabilità registrate dalla CVE Numbering Authority (CNA) <https://kernel.org/> e afferiscono dunque unicamente al kernel Linux. Maggiori informazioni a questo link: <https://www.cve.org/PartnerInformation/ListofPartners/partner/Linux>

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

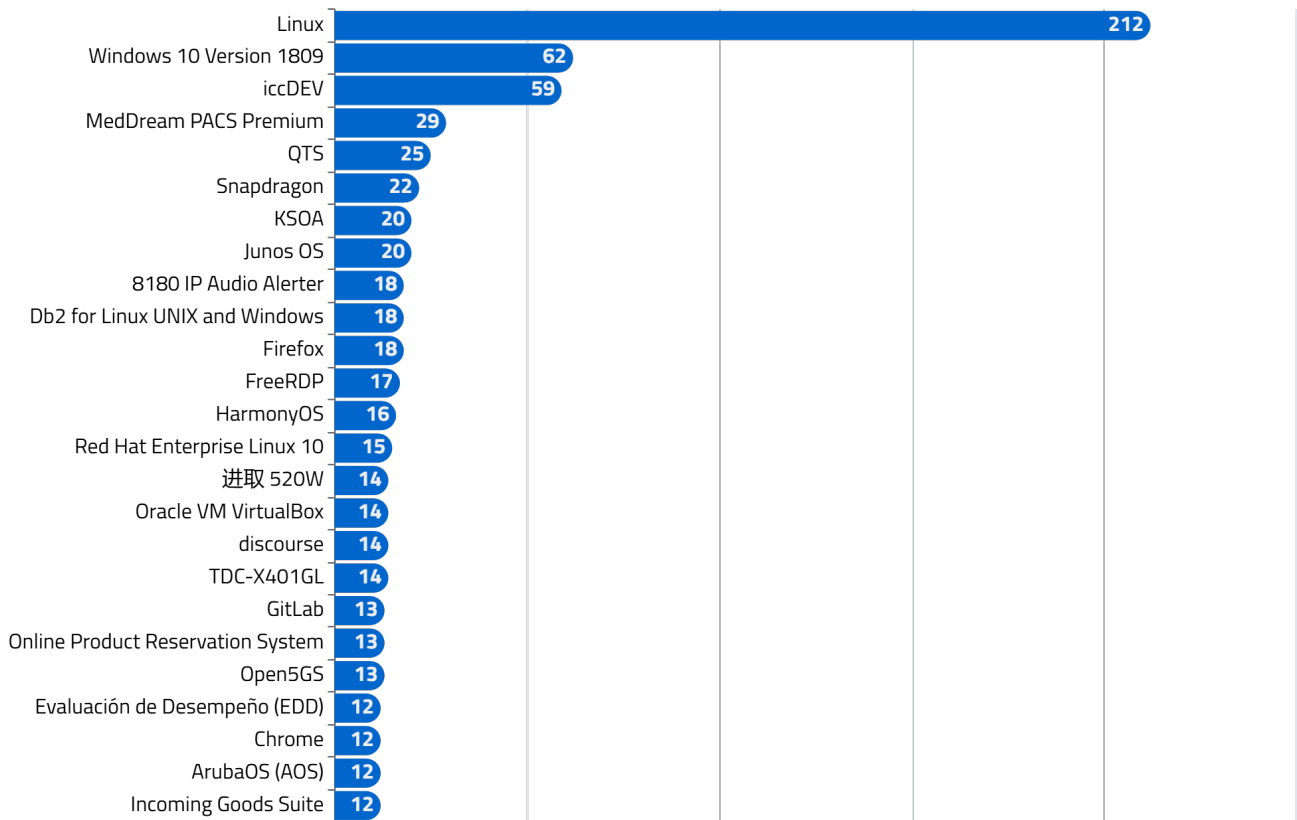


Figura 8 - top 25 prodotti affetti da vulnerabilità nel mese

3.3 CWE nel mese

In Figura 9 sono riportate le 5 tipologie di weakness (Common Weakness Enumeration – CWE) più rilevate.

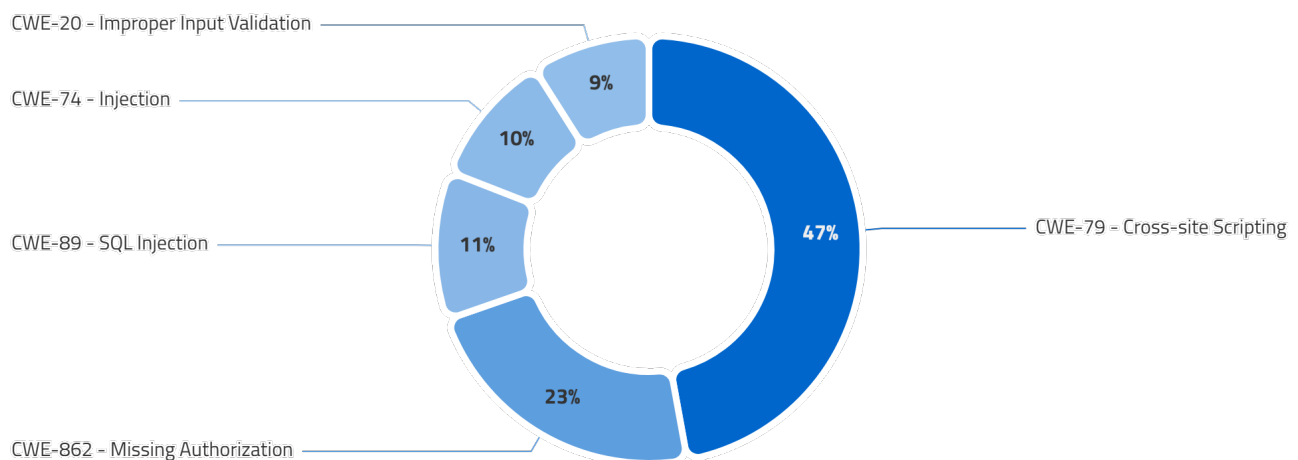


Figura 9 - top 5 CWE nel mese

3.4 Vulnerabilità con maggior probabilità di sfruttamento

Di seguito il dettaglio delle 3 vulnerabilità che potrebbero subire il maggior incremento nel trend di exploitation, ottenuto monitorando l'Exploit Prediction Scoring System (EPSS)⁷ fornito dal FIRST, nel mese in esame.

Vendor	taigaio
Prodotti e versioni vulnerabili	taiga-back tutte le versioni fino alla 6.8.3
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette ad un attaccante, se autenticato, di eseguire codice malevolo da remoto.
Data di rilascio CVE	28/10/2025 modificata il 30/10/2025
CVSS score 3.0	9 Critical
EPSS max score	0.61

Tabella 1 - CVE-2025-62368

Vendor	SmarterTools
Prodotti e versioni vulnerabili	SmarterMail tutte le versioni precedenti la build 9511
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette a un attaccante di eludere i meccanismi di autenticazione da remoto, ottenere un accesso con privilegi amministrativi ed eseguire successivamente comandi arbitrari sul server.
Data di rilascio CVE	22/01/2026 modificata il 27/01/2026
CVSS score 4.0	9.3 Critical
EPSS max score	0.55

Tabella 2 - CVE-2026-23760

⁷<https://www.first.org/epss/> fornisce un'indicazione della probabilità che una vulnerabilità venga sfruttata, è un valore aggiornato quotidianamente dal FIRST.

Vendor	n8n
Prodotti e versioni vulnerabili	n8n versioni dalla 1.65.0 fino alla 1.120.4
Descrizione vulnerabilità	Lo sfruttamento di questa vulnerabilità permette a un attaccante non autenticato di eseguire codice malevolo sul server.
Data di rilascio CVE	07/01/2026 modificata il 16/01/2026
CVSS score 3.0	10 Critical
EPSS max score	0.51

Tabella 3 - CVE-2026-21858

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 IoC⁸ condivisi dal CSIRT Italia tramite piattaforma MISP⁹, in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

A gennaio 2026, il 16% degli attacchi ransomware ha colpito soggetti critici, il 48% ha colpito soggetti a media criticità, ed il restante 36% ha coinvolto altri soggetti a criticità minore.

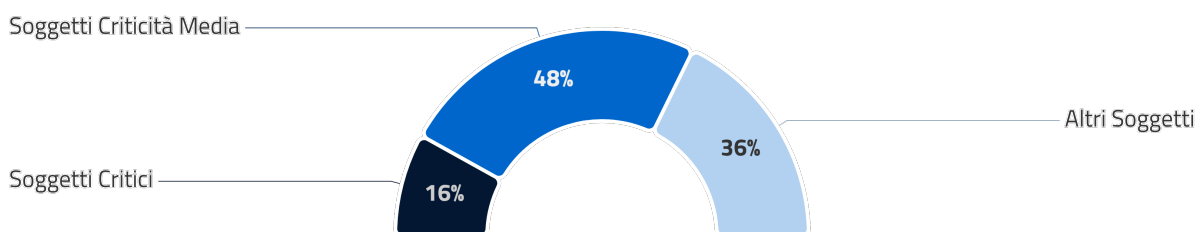


Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità

⁸IoC (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.

⁹MISP (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 mese di gennaio 2026 ha permesso di individuare **19** rivendicazioni di attacchi ransomware a danno di soggetti italiani¹⁰.

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

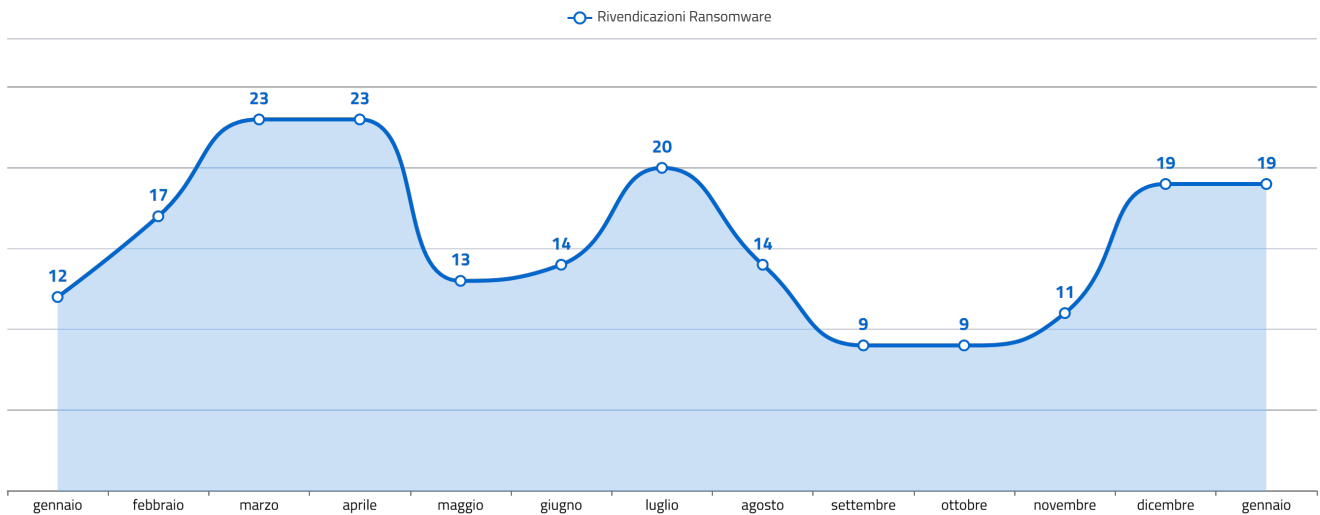


Figura 11 - andamento delle rivendicazioni Ransomware

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

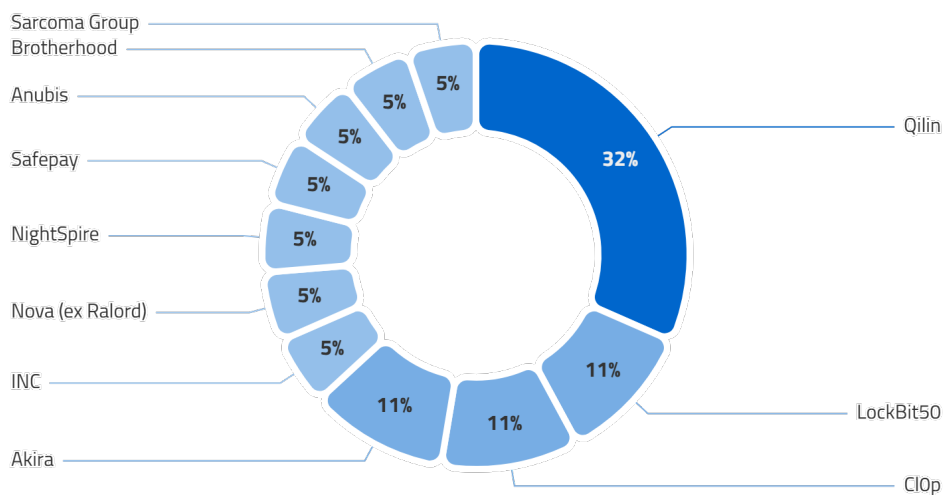


Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni

¹⁰Talvolta, le rivendicazioni relative ad attacchi ransomware non sono confermate dal soggetto coinvolto.

4.3 Rivendicazioni DDoS

A gennaio 2026 sono state individuate¹¹ 5 rivendicazioni di attacchi DDoS in danno di soggetti italiani.

Il grafico in Figura 13 mostra l'andamento delle rivendicazioni DDoS nel corso degli ultimi 12 mesi.

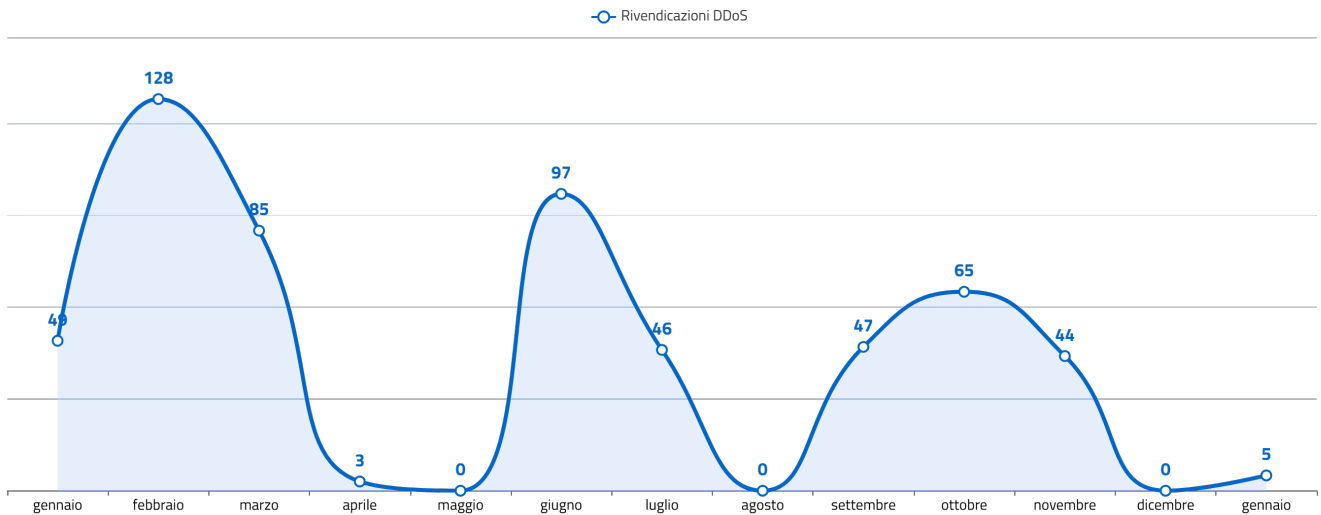


Figura 13 - andamento delle rivendicazioni DDoS

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

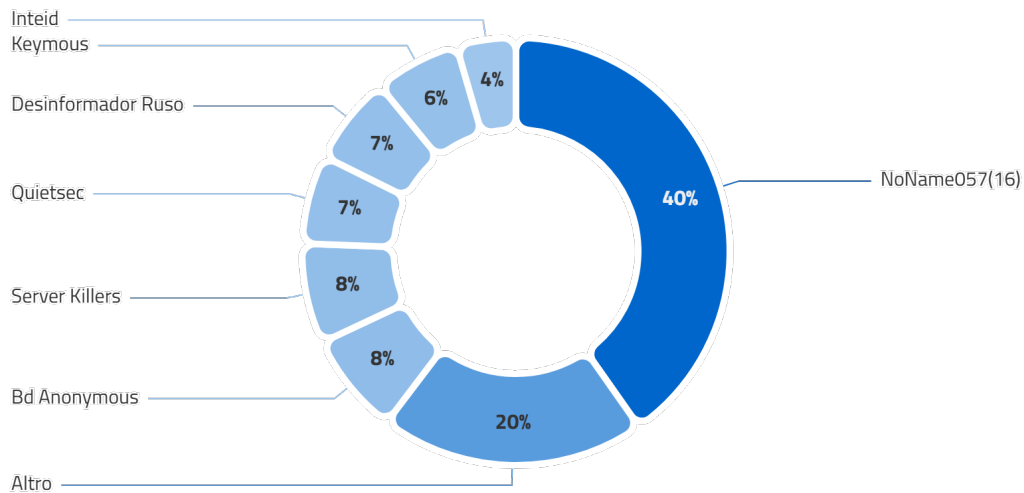


Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni

¹¹I dati rappresentano solo gli eventi pubblicamente rivendicati.

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo¹², condotte al fine di individuare e segnalare tempestivamente ai soggetti della constituency l'esposizione a specifiche minacce, rischi, vulnerabilità e criticità, che possono essere sfruttati, o che sono già in corso di sfruttamento, da parte degli attaccanti.

5.1 Comunicazioni dirette

A gennaio 2026 sono state diramate un totale di **1010** comunicazioni verso i soggetti della constituency che espongono pubblicamente su Internet complessivamente **1409** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Fortinet FortiOS, FortiProxy e FortiSwitchManager** (CVE-2025-59718): tale vulnerabilità – di tipo *Improper Verification of Cryptographic Signature* – permetterebbe a un eventuale attaccante di accedere come amministratore alla GUI o CLI del dispositivo bypassando completamente l'autenticazione FortiCloud SSO tramite un messaggio SAML malevolo, sfruttando la mancata verifica da parte dell'apparato della firma digitale del messaggio stesso.
- **Fortinet FortiManager, FortiOS, FortiProxy, FortiAnalyzer e FortiWeb** (CVE-2026-24858): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe ad un eventuale attaccante, con un account FortiCloud e un dispositivo registrato, di accedere ad altri dispositivi registrati ad account differenti, se l'autenticazione FortiCloud SSO è abilitata su tali dispositivi. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration Suite** (CVE-2025-68645): tale vulnerabilità – di tipo *Local File Inclusion* – permetterebbe a un eventuale attaccante di leggere, scrivere ed eseguire contenuti arbitrari all'interno del server target. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **SmarterTools SmarterMail** (CVE-2025-52691): tale vulnerabilità – di tipo *Arbitrary File Upload* – permetterebbe a un eventuale attaccante di caricare file arbitrari in qualsiasi posizione del server di posta, consentendo l'esecuzione

¹²Il monitoraggio individua dispositivi, servizi, asset ed errate configurazioni che incrementano la superficie di attacco sfruttabile da attori malevoli per penetrare all'interno della rete delle vittime.

di codice remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **Fortinet FortiSwitchManager e FortiOS** (CVE-2025-25249): tale vulnerabilità – di tipo *Command Execution* – permetterebbe a un eventuale attaccante di eseguire codice da remoto sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **N8n** (CVE-2026-0863, CVE-2026-1470): tali vulnerabilità – entrambe di tipo *Code Injection* – permetterebbero ad un eventuale attaccante autenticato con privilegi minimi, di eseguire codice arbitrario remoto o locale sul sistema host, con permessi del processo n8n.
- **SmarterTools SmarterMail** (CVE-2026-23760): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante di eludere i meccanismi di autenticazione, ottenere accesso come amministratore ed eseguire successivamente comandi arbitrari sul sistema operativo
Tramite ricerche passive effettuate sulle fonti a disposizione, risulterebbe a questo CSIRT che codesta Organizzazione faccia verosimilmente uso di una versione vulnerabile del prodotto in oggetto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Enhancesoft osTicket** (CVE-2026-22200): tale vulnerabilità – di tipo *Injection* – permetterebbe a un eventuale attaccante la lettura di file locali sensibili tramite la manipolazione del ticket HTML, il quale può essere esportato in un file PDF all'interno del quale vengono inclusi in formato bitmap i file di interesse.
- **N8n** (CVE-2026-21877, CVE-2025-68668, CVE-2026-21858): tali vulnerabilità – rispettivamente di tipo *Code Injection*, *Protection Mechanism Failure* e *Improper Input Validation* – permetterebbe ad un eventuale attaccante, di eseguire codice arbitrario remoto o locale, sul sistema host, con permessi del processo n8n. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle HTTP Server e Weblogic Server Proxy Plug-in** (CVE-2026-21962): tale vulnerabilità – di tipo *Improper Access Control* – permetterebbe a un eventuale attaccante di creare, cancellare, modificare o leggere dati critici sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ivanti Endpoint Manager Mobile** (CVE-2026-1340, CVE-2026-1281): tali vulnerabilità – di tipo *Code Injection* – permetterebbero a un eventuale attaccante di inviare payload contenenti comandi di sistema in quanto le componenti *In House Application Distribution* e *Android File Transfer Configuration* accettano input da richieste HTTP che non vengono correttamente sanitizzate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Veeam Backup & Replication** (CVE-2025-59470, CVE-2025-59469, CVE-2025-55125): tali vulnerabilità – di tipo *Remote Code Execution* (CVE-2025-59470 e CVE-2025-55125) e *Arbitrary File Write* (CVE-2025-59469) – permetterebbero a un attaccante di scrivere file arbitrari ed eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **N8n** (CVE-2025-68668): tale vulnerabilità – di tipo "*Protection Mechanism Failure*" – permetterebbe ad un utente autenticato con permessi di creazione e modifica dei flussi di lavoro potrebbe sfruttare questa vulnerabilità per eseguire comandi arbitrari sul sistema host con privilegi del processo n8n. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Craft CMS** (CVE-2025-68455, CVE-2025-68437, CVE-2025-68454): tali vulnerabilità – rispettivamente di tipo *Improper Neutralization*, *Unsafe Reflection* e *Server-Side Request Forgery* – permetterebbero a un eventuale attaccante tramite richieste opportunamente predisposte, di accedere a informazioni sensibili sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Appsmith** (CVE-2026-22794): tale vulnerabilità – di tipo *Origin Validation Error* – permetterebbe a un eventuale attaccante di ottenere il token di autenticazione e potenzialmente prendere il controllo dell'account.
- **Coolabs.io Coolify** (CVE-2025-64419, CVE-2025-64420, CVE-2025-64424): tali vulnerabilità – rispettivamente di

tipo *Command Injection* e *Insufficiently Protected Credentials* – permetterebbero a un eventuale attaccante di accedere a informazioni sensibili e/o eseguire codice arbitrario remoto sul sistema target. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

- **Adonisjs core** (CVE-2026-21440): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante remoto la scrittura di file su location arbitrarie del filesystem del server target.
- **Fortinet FortiSIEM** (CVE-2025-64155): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante di eseguire codice non autorizzato o comandi arbitrari mediante richieste TCP sul sistema target. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Cisco Unified Communications Manager, Unified Communications Manager IM and Presence Service e Unity Connection** (CVE-2026-20045): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire comandi arbitrari sul sistema operativo sottostante del dispositivo target. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **SolarWinds Web Help Desk** (CVE 2025 40537, CVE 2025 40536, CVE 2025 40551): 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.
- **Cal.com** (CVE-2026-23478): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante di eludere i meccanismi di autenticazione e ottenere accesso all’account di qualsiasi utente. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.

In Figura 15 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto.

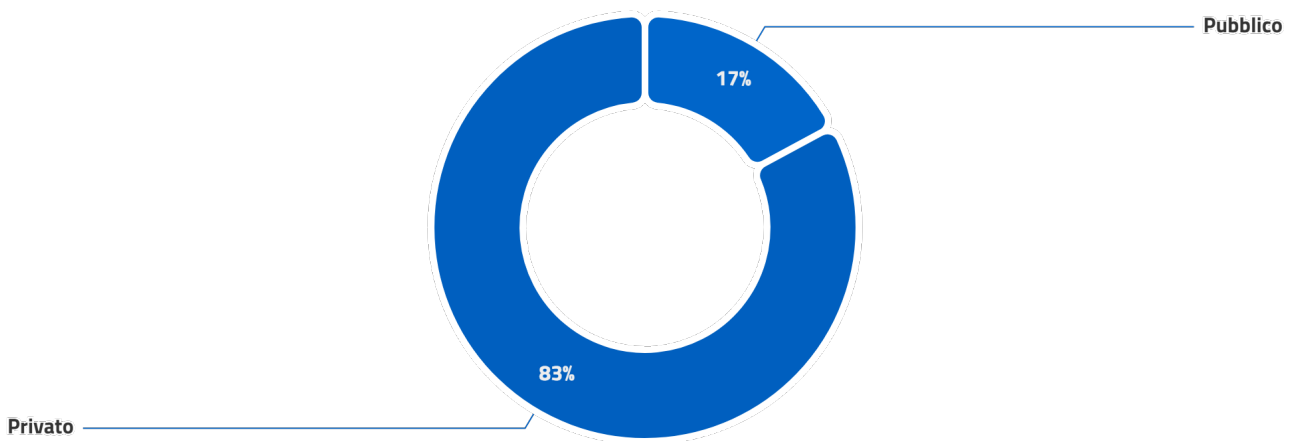


Figura 15 - distribuzione delle segnalazioni per tipologia di soggetto



**Agenzia per la
Cybersicurezza Nazionale**



OPERATIONAL SUMMARY
gennaio 2026