



# LA SETTIMANA CIBERNETICA

02 - 08 SETTEMBRE 2024



 06 SETTEMBRE 2024

## Vulnerabilità in prodotti SonicWall (AL02/240823/CSIRT-ITA) - Aggiornamento

Rilevata una vulnerabilità con gravità "alta" in diversi prodotti SonicWall. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato il bypass dei meccanismi di autenticazione sui dispositivi target e, in particolari condizioni, di compromettere la disponibilità del servizio.

[CVE-2024-40766](#)

[LEGGI DI PIÙ →](#)

 06 SETTEMBRE 2024

## Aggiornamenti per Kibana (AL04/240906/CSIRT-ITA)

Elastic NV rilascia aggiornamenti di sicurezza per sanare due vulnerabilità con gravità "critica" in Kibana, nota piattaforma di visualizzazione dati. Tali vulnerabilità, qualora sfruttate, potrebbero permettere, a un utente malintenzionato, l'esecuzione di codice arbitrario sui sistemi interessati.

[CVE-2024-37288](#)

[CVE-2024-37285](#)

[LEGGI DI PIÙ →](#)

 06 SETTEMBRE 2024

## Aggiornamenti per prodotti Trend Micro (AL03/240906/CSIRT-ITA)

Sanata una vulnerabilità, con gravità "alta", inerente al prodotto Antivirus One per macOS, soluzione di sicurezza degli endpoint sviluppata da Trend Micro.

[CVE-2024-45335](#)

[LEGGI DI PIÙ →](#)

 06 SETTEMBRE 2024

## Molteplici vulnerabilità in vari prodotti Veeam

(AL02/240906/CSIRT-ITA)

Veeam ha reso noto, tramite un bollettino di sicurezza, la presenza di molteplici vulnerabilità in alcuni dei suoi prodotti, di cui 5 con gravità "critica".

[CVE-2024-40711](#)

[CVE-2024-40713](#)

[CVE-2024-40710](#)

[CVE-2024-39718](#)

[CVE-2024-40714](#)

[CVE-2024-40712](#)

[CVE-2024-40709](#)

[CVE-2024-42024](#)

[CVE-2024-42019](#)

[CVE-2024-42023](#)

[CVE-2024-42021](#)

[CVE-2024-42022](#)

[CVE-2024-42020](#)

[CVE-2024-38650](#)

[CVE-2024-39714](#)

[CVE-2024-39715](#)

[CVE-2024-38651](#)

[CVE-2024-40718](#)

[LEGGI DI PIÙ →](#)

 06 SETTEMBRE 2024

## Risolve vulnerabilità su Zimbra Collaboration

(AL01/240906/CSIRT-ITA)

Rilasciati aggiornamenti di sicurezza per sanare molteplici vulnerabilità riscontrate nelle versioni Joule, Kepler e Daffodil di Zimbra Collaboration Suite (ZCS), nota piattaforma di collaborazione e-mail sviluppata da Synacor Inc.

[CVE-2024-27443](#)

[CVE-2024-33535](#)

[CVE-2024-33536](#)

[CVE-2024-38356](#)

[CVE-2024-45194](#)

[CVE-2024-45510](#)

[CVE-2024-45511](#)

[CVE-2024-45512](#)

[CVE-2024-45513](#)

[CVE-2024-45514](#)

[CVE-2024-45515](#)

[CVE-2024-45516](#)

[CVE-2024-45517](#)

[CVE-2024-45518](#)

[CVE-2024-45519](#)

[LEGGI DI PIÙ →](#)

 05 SETTEMBRE 2024

## Aggiornamenti di sicurezza per dispositivi Google Pixel

(AL03/240905/CSIRT-ITA)

Aggiornamenti di sicurezza Google di settembre risolvono 6 vulnerabilità nei dispositivi Pixel.

[CVE-2024-44092](#)

[CVE-2024-44093](#)

[CVE-2024-44094](#)

[CVE-2024-44095](#)

[CVE-2024-29779](#)

[CVE-2024-44096](#)

[LEGGI DI PIÙ →](#)

 05 SETTEMBRE 2024

## Aggiornamenti per prodotti Zyxel (AL03/240903/CSIRT-ITA) - Aggiornamento

Zyxel rilascia aggiornamenti di sicurezza per sanare 2 vulnerabilità presenti in diverse tipologie di dispositivi di rete e firewall.

[CVE-2024-5412](#)

[CVE-2024-7261](#)

[CVE-2024-6343](#)

[CVE-2024-7203](#)

[CVE-2024-42057](#)

[CVE-2024-42058](#)

[CVE-2024-42059](#)

[CVE-2024-42060](#)

[CVE-2024-42061](#)

[LEGGI DI PIÙ →](#)

 05 SETTEMBRE 2024

## Risolta vulnerabilità in prodotti Cisco (AL02/240905/CSIRT-ITA)

Aggiornamenti di sicurezza Cisco sanano diverse vulnerabilità, di cui una con gravità "critica" e una con gravità "alta", presenti in diversi prodotti.

[CVE-2024-20439](#)

[CVE-2024-20440](#)

[CVE-2024-20430](#)

[LEGGI DI PIÙ →](#)

 05 SETTEMBRE 2024

## Risolve vulnerabilità in OpenEdge (AL01/240905/CSIRT-ITA)

Disponibili aggiornamenti di sicurezza che risolvono 3 vulnerabilità con gravità "alta" in Progress OpenEdge, nota piattaforma di sviluppo per applicazioni aziendali. Tali vulnerabilità, qualora sfruttate, potrebbero permettere a un utente malintenzionato il bypass dei meccanismi di autenticazione e di eseguire codice arbitrario sui dispositivi target.

[CVE-2024-7654](#)

[CVE-2024-7345](#)

[CVE-2024-7346](#)

[LEGGI DI PIÙ →](#)

 04 SETTEMBRE 2024

## Rilevata nuova tecnica di diffusione malware tramite GitHub (AL06/240904/CSIRT-ITA)

Ricercatori di sicurezza hanno recentemente rilevato l'utilizzo della piattaforma GitHub per la distribuzione di un malware, denominato LummaC2, volto a carpire informazioni sensibili, quali password, cookie, informazioni bancarie, carte di credito e portafogli di criptovaluta, dai dispositivi target.

[LEGGI DI PIÙ →](#)

 04 SETTEMBRE 2024

## Rilevate vulnerabilità nel router wireless DLink DIR-846 (AL05/240904/CSIRT-ITA)

Rilevate 4 vulnerabilità di sicurezza, di cui due con gravità "critica", nel router wireless D-Link DIR-846. Tali vulnerabilità, qualora sfruttate, potrebbero permettere ad un utente malintenzionato remoto l'esecuzione di comandi arbitrari sui sistemi interessati.

[CVE-2024-41622](#)

[CVE-2024-44340](#)

[CVE-2024-44341](#)

[CVE-2024-44342](#)

[LEGGI DI PIÙ →](#)

 04 SETTEMBRE 2024

## Aggiornamenti di sicurezza per prodotti Mozilla (AL04/240904/CSIRT-ITA)

Mozilla ha rilasciato aggiornamenti di sicurezza per sanare alcune vulnerabilità, di cui 4 con gravità "alta", nei prodotti Firefox, Firefox ESR e Focus per iOS.

[CVE-2024-8385](#)

[CVE-2024-8381](#)

[CVE-2024-8387](#)

[CVE-2024-8389](#)

[LEGGI DI PIÙ →](#)

 04 SETTEMBRE 2024

## Aggiornamenti di sicurezza Android

### (AL03/240904/CSIRT-ITA)

Google ha rilasciato gli aggiornamenti di sicurezza di settembre per sanare 49 vulnerabilità che interessano il sistema operativo Android.

[CVE-2024-32896](#)

[CVE-2024-40658](#)

[CVE-2024-40662](#)

[CVE-2024-40650](#)

[CVE-2024-40652](#)

[CVE-2024-40654](#)

[CVE-2024-40655](#)

[CVE-2024-40657](#)

[CVE-2024-40656](#)

[CVE-2024-40659](#)

[CVE-2024-36972](#)

[CVE-2024-3655](#)

[CVE-2024-23716](#)

[CVE-2024-31336](#)

[CVE-2024-39431](#)

[CVE-2024-39432](#)

[CVE-2024-33042](#)

[CVE-2024-33052](#)

[CVE-2024-33034](#)

[CVE-2024-33035](#)

[CVE-2024-33038](#)

[CVE-2024-33043](#)

[CVE-2024-33045](#)

[CVE-2024-33048](#)

[CVE-2024-33050](#)

[CVE-2024-33054](#)

[CVE-2024-33057](#)

[CVE-2024-33060](#)

[CVE-2024-23358](#)

[CVE-2024-23359](#)

[CVE-2024-23362](#)

[CVE-2024-23364](#)

[CVE-2024-23365](#)

[CVE-2024-33016](#)

[CVE-2024-33051](#)

[CVE-2023-40119](#)

[CVE-2024-40678](#)

[CVE-2024-43069](#)

[CVE-2024-43070](#)

[CVE-2024-43071](#)

[CVE-2024-43074](#)

[CVE-2024-43075](#)

[CVE-2024-43076](#)

[CVE-2024-43078](#)

[CVE-2024-23694](#)

[CVE-2024-43068](#)

[CVE-2024-43072](#)

[CVE-2024-43073](#)

[CVE-2024-43079](#)

[LEGGI DI PIÙ →](#)

 04 SETTEMBRE 2024

## Sanate vulnerabilità in Apache OFBiz

### (AL02/240904/CSIRT-ITA)

Risolte due vulnerabilità, di cui una con gravità "alta", nel prodotto OFBiz di Apache Software Foundation. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione di codice arbitrario sui sistemi interessati e l'accesso a informazioni sensibili.

[CVE-2024-45507](#)

[CVE-2024-45195](#)

[LEGGI DI PIÙ →](#)



04 SETTEMBRE 2024

## Risolve vulnerabilità in Django

(AL01/240904/CSIRT-ITA)

Disponibile aggiornamento di sicurezza che risolve 2 vulnerabilità, di cui una con gravità "alta", in Django, noto framework open source per lo sviluppo di applicazioni web. Tale vulnerabilità, qualora sfruttata, potrebbe permettere la compromissione della disponibilità del servizio sulle istanze interessate.

[CVE-2024-45230](#)

[LEGGI DI PIÙ →](#)



03 SETTEMBRE 2024

## Risolve vulnerabilità in VMware Fusion

(AL04/240903/CSIRT-ITA)

VMware ha rilasciato un aggiornamento di sicurezza per sanare una vulnerabilità con gravità "alta" nel prodotto Fusion, software di virtualizzazione per macOS.

[CVE-2024-38811](#)

[LEGGI DI PIÙ →](#)



03 SETTEMBRE 2024

## Risolve vulnerabilità in Google Chrome

(AL02/240903/CSIRT-ITA)

Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 4 vulnerabilità di sicurezza, di cui 2 con gravità "alta".

[CVE-2024-8362](#)

[CVE-2024-7970](#)

[LEGGI DI PIÙ →](#)

 03 SETTEMBRE 2024

## Risolve vulnerabilità in MISP

### (AL01/240903/CSIRT-ITA)

Rilevate due nuove vulnerabilità con gravità "alta" in MISP (Malware Information Sharing Platform), nota piattaforma open source per lo scambio delle informazioni, arricchimento e correlazione dei dati esterni.

[CVE-2024-33855](#)

[CVE-2024-45509](#)

[LEGGI DI PIÙ →](#)

 02 SETTEMBRE 2024

## Vulnerabilità in Moodle

### (AL04/240822/CSIRT-ITA) - Aggiornamento

Rilevate 16 nuove vulnerabilità in Moodle, nota piattaforma open source tipicamente utilizzata per l'erogazione di corsi in modalità e-learning, di cui 1 con gravità "critica" e 7 con gravità "alta".

[CVE-2024-43440](#)

[CVE-2024-43436](#)

[CVE-2024-43428](#)

[CVE-2024-43426](#)

[CVE-2024-43425](#)

[CVE-2024-43427](#)

[CVE-2024-43430](#)

[CVE-2024-43432](#)

[LEGGI DI PIÙ →](#)