LA SETTIMANA CIBERNETICA

02 - 08 DICEMBRE 2024

06 DICEMBRE 2024

Vulnerabilità in prodotti QNAP

(AL04/241206/CSIRT-ITA)

Aggiornamenti di sicurezza QNAP risolvono 10 vulnerabilità, di cui 4 con gravità "alta", in vari prodotti.

CVE-2024-48863 CVE-2024-48865 CVE-2024-48868 CVE-2024-50393

LEGGI DI PIÙ →

06 DICEMBRE 2024

Google: aggiornamenti di sicurezza per dispositivi Pixel

(AL03/241206/CSIRT-ITA)

Aggiornamenti di sicurezza Google di dicembre risolvono 14 vulnerabilità nei dispositivi Pixel.

CVE-2024-39343 CVE-2024-53842 CVE-2024-8257 CVE-2024-11624 CVE-2024-53835 CVE-2024-53840
CVE-2024-47032 CVE-2024-53833 CVE-2024-53836 CVE-2024-53837 CVE-2024-53838 CVE-2024-53841
CVE-2024-53834 CVE-2024-53839

LEGGI DI PIÙ →

06 DICEMBRE 2024

Mitel: PoC pubblico per lo sfruttamento delle CVE-2024-41713, CVE-2024-35286 e di una vulnerabilità zero-day

(AL02/241206/CSIRT-ITA)

Disponibile un Proof of Concept (PoC) per le CVE-2024-41713 e CVE-2024-35286, già sanate dal vendor, e per una vulnerabilità zero-day, presenti nel prodotto Mitel MiCollab. Tali vulnerabilità, che riguardano il componente NuPoint Unified Messaging (NPM) di Mitel MiCollab, qualora sfruttate in combinazione, potrebbero consentire l'esecuzione di operazioni arbitrarie sul relativo database, il bypass dei meccanismi di autenticazione e l'accesso arbitrario di file sui dispositivi interessati.

CVE-2024-41713 CVE-2024-35286

LEGGI DI PIÙ →

06 DICEMBRE 2024

Vulnerabilità in prodotti SonicWall

(AL01/241206/CSIRT-ITA)

Rilevate alcune vulnerabilità, di cui 3 con gravità "alta", nei prodotti Secure Mobile Access (SMA) della serie 100 di SonicWall. Tali vulnerabilità, qualora sfruttate, potrebbero permettere a un utente malintenzionato remoto di eseguire codice arbitrario o di causare l'indisponibilità del servizio sui dispositivi target.

CVE-2024-40763 CVE-2024-45318 CVE-2024-53703

LEGGI DI PIÙ →

05 DICEMBRE 2024

Vulnerabilità in Zabbix

(AL01/241202/CSIRT-ITA) - Aggiornamento

Rilevate alcune nuove vulnerabilità, di cui 2 con gravità "critica" e 2 con gravità "alta", in Zabbix, noto prodotto open source per il monitoraggio di reti e sistemi informatici.

CVE-2024-42330 CVE-2024-42327 CVE-2024-36467 CVE-2024-36466

LEGGI DI PIÙ →

05 DICEMBRE 2024

Risolte vulnerabilità in MISP

(AL04/241205/CSIRT-ITA)

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

CVE-2024-54674 CVE-2024-54675

LEGGI DI PIÙ →

05 DICEMBRE 2024

Risolta vulnerabilità in SailPoint IdentityIQ

(AL03/241205/CSIRT-ITA)

Disponibile aggiornamento di sicurezza che risolve una vulnerabilità con gravità "critica" nel prodotto IdentityIQ, soluzione di gestione delle identità e degli accessi (IAM) di SailPoint. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malevolo l'accesso a informazioni sensibili e il bypass delle funzionalità di sicurezza sui sistemi interessati.

CVE-2024-10905

LEGGI DI PIÙ →

05 DICEMBRE 2024

Vulnerabilità in Solarwinds

(AL02/241205/CSIRT-ITA)

Risolta 1 vulnerabilità di sicurezza, con gravità "alta", in SolarWinds Platform. Tale vulnerabilità potrebbe consentire a un utente malintenzionato, qualora autenticato, di eseguire codice arbitrario sui sistemi interessati.

CVE-2024-45717

LEGGI DI PIÙ →

05 DICEMBRE 2024

Risolte vulnerabilità in Django

(AL01/241205/CSIRT-ITA)

Disponibile aggiornamento di sicurezza che risolve 2 vulnerabilità, di cui una con gravità "critica", in Django, noto framework open source per lo sviluppo di applicazioni web. Nel dettaglio la vulnerabiltià con gravità "critica" riguarda la funzionalità "lookup HasKey", utilizzata per verificare la presenza di una chiave in un campo JSON: tramite l'utilizzo di dati opportunamente predisposti risulterebbe possibile la manipolazione del valore lhs (left-hand side) dell'espressione di lookup al fine di iniettare codice SQL malevolo sulle istanze interessate.

CVE-2024-53907 CVE-2024-53908

LEGGI DI PIÙ →

04 DICEMBRE 2024

Vulnerabilità in Veeam Service Provider Console

(AL03/241204/CSIRT-ITA)

Veeam ha reso noto, tramite un bollettino di sicurezza, la presenza di due vulnerabilità, di cui una con gravità "critica" e una con gravità "alta", in Service Provider Console.

CVE-2024-42448 CVE-2024-42449

LEGGI DI PIÙ →

04 DICEMBRE 2024

Rilevato sfruttamento in rete della CVE-2024-11667 in firewall Zyxel

(AL02/241204/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-11667 – già sanata dal vendor in data 21 novembre 2024 – presente nell'interfaccia di gestione di alcuni firewall di Zyxel. Tale vulnerabilità potrebbe consentire a un utente malintenzionato il download/upload di file sui sistemi interessati.

CVE-2024-11667

LEGGI DI PIÙ →

04 DICEMBRE 2024

Vulnerabilità in Progress WhatsUp Gold

(AL01/240925/CSIRT-ITA) - Aggiornamento

Rilevate 6 vulnerabilità di sicurezza con gravita "critica" e "alta" nel prodotto WhatsUp Gold di Progress, software per il monitoraggio di infrastrutture IT.

CVE-2024-8785 CVE-2024-46908 CVE-2024-46907 CVE-2024-46906 CVE-2024-46905 CVE-2024-46909

LEGGI DI PIÙ →

04 DICEMBRE 2024

Risolte vulnerabilità in Google Chrome

(AL01/241204/CSIRT-ITA)

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

CVE-2024-12053

LEGGI DI PIÙ →

03 DICEMBRE 2024

Campagna malevola a tema Arma dei Carabinieri

(AL02/241203/CSIRT-ITA)

È stata recentemente rilevata una campagna malevola, veicolata via e-mail, che sfrutta il nome e il logo dell’Arma dei Carabinieri.

LEGGI DI PIÙ →

03 DICEMBRE 2024

Aggiornamenti di sicurezza Android

(AL01/241203/CSIRT-ITA)

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

CVE-2024-43762 CVE-2024-43764 CVE-2024-43769 CVE-2024-43767 CVE-2024-43097 CVE-2024-43768

LEGGI DI PIÙ →