LA SETTIMANA CIBERNETICA

18 - 24 NOVEMBRE 2024

22 NOVEMBRE 2024

Rilevata vulnerabilità in 7-Zip

(AL01/241122/CSIRT-ITA)

Rilasciati dettagli in merito a una vulnerabilità di sicurezza – già sanata dal vendor a giugno 2024 – presente nel noto software di compressione e archiviazione file open source 7-Zip. Tale vulnerabilità potrebbe essere sfruttata da un utente malintenzionato remoto per eseguire codice arbitrario sui sistemi interessati.

CVE-2024-11477

LEGGI DI PIÙ →

21 NOVEMBRE 2024

Rilevate vulnerabilità in Needrestart

(AL03/241121/CSIRT-ITA)

Rilevate 5 vulnerabilità di sicurezza, di cui 4 con gravità "alta", in Needrestart, utilità installata di default nei server Ubuntu, utilizzata per determinare se è necessario un riavvio del sistema o dei suoi servizi. Tali vulnerabilità, qualora sfruttate, potrebbero consentire l'esecuzione di comandi arbitrari sui sistemi interessati.

CVE-2024-48990 CVE-2024-48991 CVE-2024-48992 CVE-2024-11003

LEGGI DI PIÙ →

21 NOVEMBRE 2024

Aggiornamenti Drupal

(AL02/241121/CSIRT-ITA)

Aggiornamenti di sicurezza risolvono diverse vulnerabilità, in Drupal. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione di codice da remoto e/o il bypass dei meccanismi di sicurezza sui sistemi target.

LEGGI DI PIÙ →

21 NOVEMBRE 2024

Rilevata vulnerabilità in prodotti Atlassian

(AL01/241121/CSIRT-ITA)

Aggiornamenti di sicurezza sanano molteplici vulnerabilità in vari prodotti. Tra queste se ne evidenzia una con gravità “alta” presente nel prodotto Sourcetree, client gratuito per Git e Mercurial sviluppato da Atlassian, che offre un'interfaccia grafica per gestire i repository di codice. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto l’esecuzione di codice arbitrario sui prodotti interessati.

CVE-2024-21697

LEGGI DI PIÙ →

20 NOVEMBRE 2024

Aggiornamenti per prodotti Zyxel

(AL03/240903/CSIRT-ITA) - Aggiornamento

Zyxel rilascia aggiornamenti di sicurezza per sanare varie 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 →

20 NOVEMBRE 2024

Citrix: PoC pubblico per lo sfruttamento della CVE-2024-8069

(AL02/241114/CSIRT-ITA) - Aggiornamento

Disponibile un Proof of Concept (PoC) per la CVE-2024-8069 – già sanata dal vendor – presente in Citrix Session Recording, funzionalità di sicurezza che consente di registrare l’attività su schermo delle sessioni utente ospitate su Citrix Virtual Apps and Desktops. Tale vulnerabilità, qualora sfruttata, potrebbe permettere a un utente remoto malintenzionato l’esecuzione di codice arbitrario sui dispositivi interessati.

CVE-2024-8069

LEGGI DI PIÙ →

20 NOVEMBRE 2024

Risolte vulnerabilità in Google Chrome

(AL04/241120/CSIRT-ITA)

Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 3 vulnerabilità di sicurezza, di cui una con gravità "alta".

CVE-2024-11395

LEGGI DI PIÙ →

20 NOVEMBRE 2024

Rilevata nuova campagna di smishing a tema INPS

(AL03/241120/CSIRT-ITA)

È stato rilevato il riacutizzarsi di una campagna di smishing che sfrutta nomi e loghi riferibili ai servizi erogati dall'Istituto Nazionale della Previdenza Sociale.

LEGGI DI PIÙ →

20 NOVEMBRE 2024

Vulnerabilità in prodotti Trend Micro

(AL02/241120/CSIRT-ITA)

Sanata una vulnerabilità di gravità "alta" realtiva a Deep Security Agent e Deep Security Notifier on DSVA di Trend Micro. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto di eseguire codice arbitrario sui sistemi target.

CVE-2024-51503

LEGGI DI PIÙ →

20 NOVEMBRE 2024

Apple: rilevato sfruttamento in rete delle vulnerabilità CVE-2024-44308 e CVE-2024-44309

(AL01/241120/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete di 2 vulnerabilità che interessano vari prodotti Apple. Tali vulnerabilità potrebbero permettere di eseguire codice da remoto e di perpetrare attacchi di tipo Cross Site Scripting (XSS) tramite risorse web opportunamente predisposte.

CVE-2024-44308 CVE-2024-44309

LEGGI DI PIÙ →

19 NOVEMBRE 2024

Vulnerabilità in Apache Tomcat

(AL03/241119/CSIRT-ITA)

Rilevate 3 vulnerabilità di sicurezza, di cui una con gravità "critica", nel noto server web open source sviluppato da Apache Software Foundation. Tale vulnerabilità, qualora sfruttata, potrebbe permettere a un utente malintenzionato il bypass dei meccanismi di autenticazione sui dispositivi target.

CVE-2024-52316

LEGGI DI PIÙ →

19 NOVEMBRE 2024

Oracle: rilevato lo sfruttamento in rete della CVE-2024-21287

(AL02/241119/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-21287 che interessa il prodotto Agile Product Lifecycle Management (PLM), soluzione progettata per la gestione del ciclo di vita dei prodotti, dalla concezione iniziale fino alla dismissione. Tale vulnerabilità, con score cvss v3.x pari a 7.5, potrebbe permettere la divulgazione di file contenenti informazioni sensibili presenti sui sistemi target.

CVE-2024-21287

LEGGI DI PIÙ →

19 NOVEMBRE 2024

Aggiornamenti per prodotti Siemens

(AL01/241119/CSIRT-ITA)

Siemens ha rilasciato aggiornamenti di sicurezza per correggere vulnerabilità in alcuni dei prodotti delle serie Siveillance Video, - soluzione per la gestione video (VMS) - Tecnomatix Plant Simulation - software di simulazione e ottimizzazione della produzione - e SINEC INS - software per la gestione centralizzata dei servizi di rete industriali.

CVE-2024-0056 CVE-2024-46888 CVE-2024-46890 CVE-2024-52565 CVE-2024-52566 CVE-2024-52567 CVE-2024-52568 CVE-2024-52569 CVE-2024-52570 CVE-2024-52571 CVE-2024-52572 CVE-2024-52573 CVE-2024-52574

LEGGI DI PIÙ →

19 NOVEMBRE 2024

Palo Alto Networks: rilevato sfruttamento in rete di una vulnerabilità nel software PAN-OS

(AL02/241115/CSIRT-ITA) - Aggiornamento

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-0012 che interessa l'interfaccia di gestione del software PAN-OS di alcuni firewall Palo Alto Networks. Tale vulnerabilità, di tipo "Authentication Bypass", potrebbe consentire ad un utente malevolo non autenticato, con accesso alla rete, di ottenere privilegi amministrativi sull'interfaccia di gestione, di alterare la configurazione e di eseguire comandi arbitrari sui sistemi target.

CVE-2024-0012

LEGGI DI PIÙ →

19 NOVEMBRE 2024

Risolte vulnerabilità in prodotti VMware

(AL01/240918/CSIRT-ITA) - Aggiornamento

VMware ha rilasciato aggiornamenti di sicurezza per sanare alcune vulnerabilità, di cui una con gravità "critica" nei prodotti vCenter Server e Cloud Foundation, noto software di virtualizzazione.

CVE-2024-38812 CVE-2024-38813

LEGGI DI PIÙ →