LA SETTIMANA CIBERNETICA

11 - 17 NOVEMBRE 2024

15 NOVEMBRE 2024

Rilevate vulnerabilità in PostgreSQL

(AL03/241115/CSIRT-ITA)

PostgreSQL Global Development Group ha rilasciato aggiornamenti di sicurezza per risolvere 4 vulnerabilità, di cui una con gravità "alta" in PostgreSQL PL/Perl, linguaggio procedurale che permette di scrivere funzioni e procedure in PostgreSQL utilizzando il linguaggio di programmazione Perl. Tale vulnerabilità potrebbe essere sfruttata da un utente malevolo per modificare le variabili d'ambiente del sistema target al fine di eseguire codice arbitrario.

CVE-2024-10979

LEGGI DI PIÙ →

15 NOVEMBRE 2024

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

(AL02/241115/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete di una vulnerabilità che interessa l'interfaccia di gestione del software PAN-OS di alcuni firewall Palo Alto Networks. Tale vulnerabilità, di tipo "Unauthenticated Remote Command Execution", potrebbe consentire ad un utente malevolo remoto la possibilità di eseguire comandi arbitrari sui sistemi target.

LEGGI DI PIÙ →

15 NOVEMBRE 2024

Palo Alto Networks: PoC pubblico per lo sfruttamento di vulnerabilità in prodotti firewall

(AL02/241010/CSIRT-ITA) - Aggiornamento

Palo Alto Networks ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità. In particolare, per 5 di tali vulnerabilità – che interessano la soluzione Network Expedition - risulterebbe disponibile un Proof of Concept (PoC) che potrebbe permettere lo sfruttamento concatenato delle stesse al fine di prendere il controllo degli account di amministrazione dei prodotti firewall.

CVE-2024-9463 CVE-2024-9464 CVE-2024-9465 CVE-2024-9466 CVE-2024-9467 CVE-2024-9468

LEGGI DI PIÙ →

15 NOVEMBRE 2024

Smishing: nuova campagna a tema Hype

(AL01/241115/CSIRT-ITA)

Questo CSIRT ha recentemente rilevato un riacutizzarsi di una campagna di phishing a tema Hype, perpetrata via SMS (smishing), volta a carpire le credenziali d'accesso ai servizi bancari delle potenziali vittime.

LEGGI DI PIÙ →

14 NOVEMBRE 2024

Vulnerabilità in Zoom

(AL04/241114/CSIRT-ITA)

Rilevate 6 nuove vulnerabilità, di cui 2 con gravità "alta" in prodotti Zoom. Tali vulnerabilità potrebbero permettere l'ottenimento di privilegi elevati e/o il bypass dei meccanismi di sicurezza sulle istanze interessate.

CVE-2024-45419 CVE-2024-45421

LEGGI DI PIÙ →

14 NOVEMBRE 2024

Palo Alto Networks risolve vulnerabilità in vari prodotti

(AL03/241114/CSIRT-ITA)

Aggiornamenti di sicurezza sanano alcune vulnerabilità, di cui 3 con gravità "alta" in PAN-OS che potrebbero comportare la compromissione della disponibilità del servizio sui sistemi interessati.

CVE-2024-9472 CVE-2024-2551 CVE-2024-2550

LEGGI DI PIÙ →

14 NOVEMBRE 2024

Citrix: PoC pubblico per lo sfruttamento della CVE-2024-8069 (AL02/241114/CSIRT-ITA)

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 →

14 NOVEMBRE 2024

Mozilla: vulnerabilità nel software Thunderbird (AL01/241114/CSIRT-ITA)

Mozilla ha rilasciato aggiornamenti di sicurezza per correggere una vulnerabilità con gravità "alta" nel noto client di posta elettronica Thunderbird, che qualora sfruttata potrebbe comportare l'esposizione di informazioni sensibili.

CVE-2024-11159

LEGGI DI PIÙ →

14 NOVEMBRE 2024

D-Link: PoC pubblico per lo sfruttamento della CVE-2024-10914 (AL01/241111/CSIRT-ITA) - Aggiornamento

Disponibile un Proof of Concept (PoC) per la vulnerabilità CVE-2024-10914 presente in alcuni modelli di NAS D-Link. Tale vulnerabilità – con score CVSS v3.x pari a 9.8 – potrebbe essere utilizzata per eseguire codice arbitrario sui dispositivi interessati tramite l'invio al NAS di una richiesta HTTP GET opportunamente predisposta.

CVE-2024-10914

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Sanate vulnerabilità su GitLab CE/EE

(AL06/241113/CSIRT-ITA)

Rilasciati aggiornamenti di sicurezza che risolvono 6 vulnerabilità, di cui una con gravità "alta", in GitLab Community Edition (CE) ed Enterprise Edition (EE).

CVE-2024-9693

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Fortinet: rilevate vulnerabilità in molteplici prodotti

(AL05/241113/CSIRT-ITA)

Rilevate nuove vulnerabilità in vari prodotti, di cui 4 con gravità "alta". Tali vulnerabilità potrebbero permettere il bypass dei meccanismi di sicurezza, l'esecuzione di comandi arbitrari e la possibilità di elevare i privilegi utente sui sistemi interessati.

CVE-2024-23666 CVE-2024-36513 CVE-2024-47574 CVE-2023-50176

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Adobe rilascia aggiornamenti per sanare molteplici vulnerabilità

(AL04/241113/CSIRT-ITA)

Adobe ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità, con gravità "alta", nei prodotti After Effects, Substance 3D Painter, Illustrator, InDesign, Photoshop e Commerce.

CVE-2024-45114 CVE-2024-47426 CVE-2024-47427 CVE-2024-47428 CVE-2024-47429 CVE-2024-47430
CVE-2024-47431 CVE-2024-47432 CVE-2024-47433 CVE-2024-47434 CVE-2024-47441 CVE-2024-47442
CVE-2024-47443 CVE-2024-47450 CVE-2024-47451 CVE-2024-47452 CVE-2024-49507 CVE-2024-49508
CVE-2024-49509 CVE-2024-49514 CVE-2024-49515 CVE-2024-49516 CVE-2024-49517 CVE-2024-49518
CVE-2024-49519 CVE-2024-49520 CVE-2024-49521 CVE-2024-49525

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Ivanti November Security Update

(AL03/241113/CSIRT-ITA)

Ivanti rilascia aggiornamenti di sicurezza che risolvono 49 vulnerabilità, di cui 9 con gravità "critica" e 36 con gravità "alta", nei prodotti EPM (Endpoint Manager), ICS (Ivanti Connect Secure), IPS (Ivanti Policy Secure), ISAC (Ivanti Secure Access Client) e Ivanti Avalanche.

CVE-2024-50330 CVE-2024-38655 CVE-2024-38656 CVE-2024-39710 CVE-2024-39711 CVE-2024-39712
CVE-2024-11007 CVE-2024-11006 CVE-2024-11005 CVE-2024-34787 CVE-2024-50322 CVE-2024-32839
CVE-2024-32841 CVE-2024-32844 CVE-2024-32847 CVE-2024-34780 CVE-2024-37376 CVE-2024-34781
CVE-2024-34782 CVE-2024-34784 CVE-2024-50323 CVE-2024-50324 CVE-2024-50326 CVE-2024-50327
CVE-2024-50328 CVE-2024-50329 CVE-2024-37400 CVE-2024-9420 CVE-2024-47906 CVE-2024-47907
CVE-2024-8495 CVE-2024-38649 CVE-2024-39709 CVE-2024-11004 CVE-2024-8539 CVE-2024-9842
CVE-2024-29211 CVE-2024-37398 CVE-2024-7571 CVE-2024-50317 CVE-2024-50318 CVE-2024-50319
CVE-2024-50320 CVE-2024-50321 CVE-2024-50331

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Vulnerabilità in prodotti Citrix

(AL02/241113/CSIRT-ITA)

Rilevate 2 nuove vulnerabilità di sicurezza, di cui una con gravità "alta", che interessa i software Citrix NetScaler ADC e Gateway. Tale vulnerabilità potrebbe permettere ad un utente malevolo di compromettere la disponibilità del servizio sui dispositivi target.

CVE-2024-8534

LEGGI DI PIÙ →

13 NOVEMBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/241113/CSIRT-ITA)

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 158 nuove vulnerabilità, di cui 4 di tipo 0-day.

LEGGI DI PIÙ →

12 NOVEMBRE 2024

Aggiornamenti per prodotti Siemens

(AL04/241112/CSIRT-ITA)

Siemens ha rilasciato aggiornamenti di sicurezza per correggere molteplici vulnerabilità nei propri prodotti – anche SCADA, di cui una con gravità "critica" in TeleControl, sistema di telecontrollo progettato per monitorare e controllare impianti industriali.

CVE-2024-44102

LEGGI DI PIÙ →

12 NOVEMBRE 2024

Rilevate vulnerabilità nel prodotto DLink DSL6740C

(AL03/241112/CSIRT-ITA)

Rilevate 7 vulnerabilità di sicurezza, di cui una con gravità "critica" e 6 con gravità "alta", nel prodotto D-Link DSL6740C. Tali vulnerabilità, qualora sfruttate, potrebbero permettere ad un utente malintenzionato remoto il bypass dei meccanismi di autenticazione e l'esecuzione di comandi arbitrari sui sistemi interessati.

CVE-2024-11068 CVE-2024-11067 CVE-2024-11066 CVE-2024-11065 CVE-2024-11064 CVE-2024-11063 CVE-2024-11062

LEGGI DI PIÙ →

12 NOVEMBRE 2024

SAP Security Patch Day

(AL02/241112/CSIRT-ITA)

SAP rilascia il Security Patch Day di novembre che risolve diverse vulnerabilità, di cui una con gravità "alta" che interessa il prodotto SAP Web Dispatcher, componente chiave per la gestione del traffico HTTP(S) verso i sistemi SAP. Tale vulnerabilità potrebbe permettere ad un utente malevolo la creazione di link opportunamente predisposti che, qualora eseguiti tramite browser (XSS) o indirizzati ai server target (SSRF), potrebbero permettere l'esecuzione di codice arbitrario sulle istanze interessate.

CVE-2024-47590

LEGGI DI PIÙ →

12 NOVEMBRE 2024

Schneider Electric: sanate vulnerabilità in vari prodotti

(AL01/241112/CSIRT-ITA)

Sanate nuove vulnerabilità presenti in alcuni prodotti – integrabili anche in soluzioni SCADA - di Schneider Electric, di cui una con gravità "critica" e 5 con gravità "alta".

CVE-2024-9409 CVE-2024-8933 CVE-2024-8935 CVE-2024-8937 CVE-2024-8938 CVE-2024-10575

LEGGI DI PIÙ →