LA SETTIMANA CIBERNETICA

09 - 15 DICEMBRE 2024

13 DICEMBRE 2024

Phishing: campagna a tema “Sondaggio Generali”

(AL01/241213/CSIRT-ITA)

Questo CSIRT ha recentemente rilevato il riacutizzarsi di una campagna di phishing a tema “sondaggio” – come già trattato da questo CSIRT nell’ambito dell’AL01/240613/CSIRT-ITA – che ripropone loghi e riferimenti inerenti la nota compagnia assicurativa Generali e volta a carpire le informazioni personali delle potenziali vittime, compresi gli estremi delle carte di credito.

LEGGI DI PIÙ →

13 DICEMBRE 2024

Rilevato sfruttamento di prodotti Cleo

(AL04/241210/CSIRT-ITA) - Aggiornamento

Rilevato lo sfruttamento attivo in rete di una vulnerabilità di tipo “Remote Code Execution” presente nei prodotti Harmony, VLTrader e LexiCom della suite Cleo, soluzioni software utilizzate principalmente per la gestione dei trasferimenti di file.

CVE-2024-50623

LEGGI DI PIÙ →

12 DICEMBRE 2024

Aggiornamenti di sicurezza Apple

(AL01/241212/CSIRT-ITA)

Apple ha rilasciato aggiornamenti di sicurezza per sanare molteplici vulnerabilità presenti nei propri prodotti.

CVE-2024-54513	CVE-2024-54486	CVE-2024-54500	CVE-2024-44245	CVE-2024-54494	CVE-2024-45490
CVE-2024-54492	CVE-2024-54501	CVE-2024-54479	CVE-2024-54502	CVE-2024-54508	CVE-2024-54505
CVE-2024-54534	CVE-2024-54526	CVE-2024-54527	CVE-2024-54510	CVE-2024-54514	CVE-2024-44225
CVE-2024-54477	CVE-2024-54529	CVE-2024-44300	CVE-2024-54466	CVE-2024-54489	CVE-2024-44201
CVE-2024-54474	CVE-2024-54476	CVE-2024-44248	CVE-2024-54528	CVE-2024-54498	CVE-2024-44291
CVE-2024-44224	CVE-2024-44220	CVE-2024-54495	CVE-2024-54490	CVE-2024-54506	CVE-2024-54531
CVE-2024-54465	CVE-2024-54491	CVE-2024-54484	CVE-2024-54504	CVE-2023-32395	CVE-2024-44246
CVE-2024-54515	CVE-2024-54524	CVE-2024-54493	CVE-2024-44243	CVE-2024-54485	CVE-2024-54503

LEGGI DI PIÙ →

11 DICEMBRE 2024

Sanate vulnerabilità su GitLab CE/EE

(AL06/241211/CSIRT-ITA)

Rilasciati aggiornamenti di sicurezza che risolvono 12 vulnerabilità, di cui due con gravità “alta”, in GitLab Community Edition (CE) ed Enterprise Edition (EE).

CVE-2024-11274	CVE-2024-8233

LEGGI DI PIÙ →

11 DICEMBRE 2024

Ivanti December Security Update

(AL05/241211/CSIRT-ITA)

Ivanti rilascia aggiornamenti di sicurezza che risolvono 11 vulnerabilità, di cui 5 con gravità "critica" e 6 con gravità "alta", nei prodotti CSA (Cloud Services Application), DSM (Desktop and Server Management), ICS (Ivanti Connect Secure), IPS (Ivanti Policy Secure), Ivanti Sentry, EPM (Endpoint Manager), iSec (Ivanti Security Controls), Patch for Configuration Manager, Neurons for Patch Management e Neurons Agent Platform.

CVE-2024-11639 CVE-2024-11772 CVE-2024-11773 CVE-2024-7572 CVE-2024-37377 CVE-2024-9844
CVE-2024-37401 CVE-2024-11633 CVE-2024-11634 CVE-2024-8540 CVE-2024-10256

LEGGI DI PIÙ →

11 DICEMBRE 2024

Adobe rilascia aggiornamenti per sanare molteplici vulnerabilità

(AL04/241211/CSIRT-ITA)

Adobe ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità, di cui 2 con gravità "critica" e 39 con gravità "alta", in molteplici prodotti.

CVE-2024-49551 CVE-2024-49552 CVE-2024-49553 CVE-2024-49538 CVE-2024-49541 CVE-2024-49537
CVE-2024-52982 CVE-2024-52983 CVE-2024-52984 CVE-2024-52985 CVE-2024-52986 CVE-2024-52987
CVE-2024-52988 CVE-2024-52989 CVE-2024-52990 CVE-2024-45155 CVE-2024-45156 CVE-2024-53953
CVE-2024-53954 CVE-2024-49543 CVE-2024-49544 CVE-2024-49545 CVE-2024-54032 CVE-2024-54034
CVE-2024-54035 CVE-2024-54036 CVE-2024-54037 CVE-2024-52994 CVE-2024-52995 CVE-2024-52996
CVE-2024-52997 CVE-2024-52999 CVE-2024-53000 CVE-2024-53001 CVE-2024-53002 CVE-2024-53003
CVE-2024-53955 CVE-2024-53956 CVE-2024-53957 CVE-2024-53958 CVE-2024-53959

LEGGI DI PIÙ →

11 DICEMBRE 2024

Rilevate vulnerabilità in prodotti Splunk

(AL03/241211/CSIRT-ITA)

Splunk ha rilasciato aggiornamenti di sicurezza per correggere alcune vulnerabilità, di cui una con gravità “alta” nel prodotto Splunk Secure Gateway.

CVE-2024-53247

LEGGI DI PIÙ →

11 DICEMBRE 2024

Risolte vulnerabilità in Google Chrome

(AL02/241211/CSIRT-ITA)

Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 3 vulnerabilità di sicurezza, di cui 2 con gravità “alta”.

CVE-2024-12381 CVE-2024-12382

LEGGI DI PIÙ →

11 DICEMBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/241211/CSIRT-ITA)

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 71 nuove vulnerabilità, di cui una di tipo 0-day.

CVE-2024-49138	CVE-2024-49101	CVE-2024-49099	CVE-2024-49126	CVE-2024-49097	CVE-2024-49075
CVE-2024-49090	CVE-2024-49081	CVE-2024-49119	CVE-2024-49116	CVE-2024-49092	CVE-2024-49110
CVE-2024-49129	CVE-2024-49096	CVE-2024-49088	CVE-2024-49083	CVE-2024-49106	CVE-2024-49057
CVE-2024-49062	CVE-2024-49068	CVE-2024-49072	CVE-2024-49132	CVE-2024-49098	CVE-2024-49059
CVE-2024-49103	CVE-2024-49093	CVE-2024-43600	CVE-2024-49142	CVE-2024-49078	CVE-2024-49122
CVE-2024-49095	CVE-2024-49069	CVE-2024-49114	CVE-2024-49121	CVE-2024-49065	CVE-2024-49086
CVE-2024-49115	CVE-2024-49079	CVE-2024-49109	CVE-2024-49087	CVE-2024-49124	CVE-2024-49080
CVE-2024-49082	CVE-2024-43594	CVE-2024-49107	CVE-2024-49127	CVE-2024-49064	CVE-2024-49070
CVE-2024-49085	CVE-2024-49073	CVE-2024-49102	CVE-2024-49117	CVE-2024-49094	CVE-2024-49128
CVE-2024-49118	CVE-2024-49084	CVE-2024-49091	CVE-2024-49112	CVE-2024-49123	CVE-2024-49104
CVE-2024-49125	CVE-2024-49108	CVE-2024-49074	CVE-2024-49076	CVE-2024-49077	CVE-2024-49113
CVE-2024-49120	CVE-2024-49063	CVE-2024-49111	CVE-2024-49089		

LEGGI DI PIÙ →

10 DICEMBRE 2024

Aggiornamenti per prodotti Siemens

(AL03/241210/CSIRT-ITA)

Siemens ha rilasciato aggiornamenti di sicurezza per correggere molteplici vulnerabilità nei propri prodotti, di cui 34 con gravità "alta".

CVE-2020-28398 CVE-2024-52051 CVE-2024-45463 CVE-2024-45464 CVE-2024-45465 CVE-2024-45466
CVE-2024-45467 CVE-2024-45468 CVE-2024-45469 CVE-2024-45470 CVE-2024-45471 CVE-2024-45472
CVE-2024-45473 CVE-2024-45474 CVE-2024-45475 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 CVE-2024-53041 CVE-2024-53242 CVE-2024-54093 CVE-2024-54094 CVE-2024-54095
CVE-2024-49849 CVE-2024-41981 CVE-2024-47046 CVE-2024-54091

LEGGI DI PIÙ →

10 DICEMBRE 2024

Schneider Electric: rilevate vulnerabilità in vari prodotti

(AL02/241210/CSIRT-ITA)

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

CVE-2024-11999 CVE-2024-11737

LEGGI DI PIÙ →

10 DICEMBRE 2024

SAP Security Patch Day

(AL01/241210/CSIRT-ITA)

SAP rilascia il Security Patch Day di dicembre che risolve diverse vulnerabilità, di cui 3 con gravità "alta".

CVE-2024-47578 CVE-2024-54197 CVE-2024-54198

LEGGI DI PIÙ →

10 DICEMBRE 2024

Rilevata vulnerabilità in 7-Zip

(AL01/241122/CSIRT-ITA) - Aggiornamento

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 →

10 DICEMBRE 2024

Vulnerabilità in prodotti QNAP

(AL01/241125/CSIRT-ITA) - Aggiornamento

Aggiornamenti di sicurezza QNAP risolvono 24 vulnerabilità, di cui 2 con gravità "critica" e 9 con gravità "alta", in vari prodotti.

CVE-2024-50396 CVE-2024-50397 CVE-2024-48862 CVE-2024-38643 CVE-2024-38644 CVE-2024-38645
CVE-2024-38646 CVE-2024-50395 CVE-2024-48860 CVE-2024-48861 CVE-2024-38647

LEGGI DI PIÙ →

10 DICEMBRE 2024

Rilevate vulnerabilità in Needrestart

(AL03/241121/CSIRT-ITA) - Aggiornamento

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 →

09 DICEMBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/240814/CSIRT-ITA) - Aggiornamento

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 85 nuove vulnerabilità, di cui 10 di tipo 0-day.

CVE-2024-38178	CVE-2024-38193	CVE-2024-38213	CVE-2024-38106	CVE-2024-38107	CVE-2024-38189
CVE-2024-38199	CVE-2024-21302	CVE-2024-38200	CVE-2024-38202	CVE-2024-38217	CVE-2024-38161
CVE-2024-38177	CVE-2024-38152	CVE-2024-38145	CVE-2024-38116	CVE-2024-38201	CVE-2024-38134
CVE-2024-38211	CVE-2024-38168	CVE-2024-38128	CVE-2024-38121	CVE-2023-40547	CVE-2024-38136
CVE-2024-38115	CVE-2024-38122	CVE-2024-38184	CVE-2024-38118	CVE-2024-38146	CVE-2024-38120
CVE-2024-38171	CVE-2024-38133	CVE-2024-38114	CVE-2024-38153	CVE-2024-38148	CVE-2024-38127
CVE-2024-38132	CVE-2024-38158	CVE-2024-37968	CVE-2024-38187	CVE-2024-38191	CVE-2024-38123
CVE-2024-38098	CVE-2024-38138	CVE-2024-38223	CVE-2024-38195	CVE-2024-38142	CVE-2024-38143
CVE-2024-38159	CVE-2024-29995	CVE-2024-38109	CVE-2024-38170	CVE-2024-38117	CVE-2024-38162
CVE-2024-38154	CVE-2022-3775	CVE-2024-38137	CVE-2024-38172	CVE-2024-38108	CVE-2024-38063
CVE-2024-38144	CVE-2024-38180	CVE-2024-38126	CVE-2024-38130	CVE-2024-38160	CVE-2024-38173
CVE-2024-38185	CVE-2024-38167	CVE-2024-38169	CVE-2024-38214	CVE-2024-38141	CVE-2024-38135
CVE-2024-38084	CVE-2024-38157	CVE-2024-38151	CVE-2024-38131	CVE-2022-2601	CVE-2024-38155
CVE-2024-38198	CVE-2024-38196	CVE-2024-38140	CVE-2024-38163	CVE-2024-38215	CVE-2024-38197
CVE-2024-38147	CVE-2024-38125	CVE-2024-38165	CVE-2024-38186	CVE-2024-38150	

LEGGI DI PIÙ →

09 DICEMBRE 2024

Sanate vulnerabilità in Qlik Sense Enterprise

(AL01/241209/CSIRT-ITA)

Sanate due vulnerabilità con gravità “alta” in Qlik Sense Enterprise, piattaforma di business intelligence e data integration. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione da remoto di codice arbitrario sui sistemi target.

CVE-2024-55579 CVE-2024-55580

LEGGI DI PIÙ →