LA SETTIMANA CIBERNETICA

16 - 22 SETTEMBRE 2024

20 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 →

20 SETTEMBRE 2024

Ivanti: rilevato sfruttamento in rete della CVE-2024-8963 relativa al prodotto Cloud Service Appliance

(AL01/240920/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-8963 – già sanata dal vendor – che interessa la soluzione Cloud Service Appliance (CSA) di Ivanti, dispositivo di rete per la gestione e la protezione dei dispositivi aziendali connessi a Internet.

CVE-2024-8963 CVE-2024-8190

LEGGI DI PIÙ →

19 SETTEMBRE 2024

SambaSpy: campagna malspam indirizzata verso utenze italiane

(BL01/240919/CSIRT-ITA)

Ricercatori di sicurezza hanno rilevato una campagna di distribuzione malware volta a distribuire il RAT SambaSpy esclusivamente verso utenze localizzate sul territorio italiano.

LEGGI DI PIÙ →

18 SETTEMBRE 2024

Aggiornamenti per Ruby-SAML

(AL05/240918/CSIRT-ITA)

Rilevata vulnerabilità – già risolta dal vendor – che interessa la libreria ruby-saml del noto linguaggio di programmazione Ruby, tipicamente utilizzata per implementare le modalità di autorizzazione SAML lato client. Tale vulnerabilità, qualora sfruttata, potrebbe consentire, a un attaccante non autenticato, di bypassare i meccanismi di sicurezza e accedere al sistema interessato.

CVE-2024-45409

LEGGI DI PIÙ →

18 SETTEMBRE 2024

Sanata vulnerabilità su GitLab CE/EE

(AL04/240918/CSIRT-ITA)

Rilasciati aggiornamenti di sicurezza che risolvono una vulnerabilità con gravità “critica” in GitLab Community Edition (CE) ed Enterprise Edition (EE).

CVE-2024-45409

LEGGI DI PIÙ →

18 SETTEMBRE 2024

Risolte vulnerabilità in Google Chrome

(AL03/240918/CSIRT-ITA)

Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 9 vulnerabilità di sicurezza, di cui una con gravità “alta”.

CVE-2024-8904

LEGGI DI PIÙ →

18 SETTEMBRE 2024

Aggiornamenti di sicurezza LibreOffice

(AL02/240918/CSIRT-ITA)

Sanata una vulnerabilità con gravità "alta" in LibreOffice, noto software di produttività open source e multipiattaforma. Tale vulnerabilità, in determinate condizioni, potrebbe permettere l'esecuzione di macro malevole tramite documenti opportunamente predisposti.

CVE-2024-7788

LEGGI DI PIÙ →

18 SETTEMBRE 2024

Risolte vulnerabilità in prodotti VMware

(AL01/240918/CSIRT-ITA)

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 →

17 SETTEMBRE 2024

Vulnerabilità in FileSender

(AL02/240917/CSIRT-ITA)

Rilevata una vulnerabilità di sicurezza, con gravità "alta" in FileSender, applicazione web open source utilizzata per inviare file di grandi dimensioni in modo sicuro.

CVE-2024-45186

LEGGI DI PIÙ →

17 SETTEMBRE 2024

Aggiornamenti di sicurezza Android

(AL01/240703/CSIRT-ITA) - Aggiornamento

Google ha rilasciato gli aggiornamenti di sicurezza di luglio per sanare 27 vulnerabilità che interessano il sistema operativo Android.

CVE-2024-23368 CVE-2024-21469 CVE-2024-21465 CVE-2024-21462 CVE-2024-21460 CVE-2024-21461
CVE-2024-23380 CVE-2024-23373 CVE-2024-23372 CVE-2024-20077 CVE-2024-26923 CVE-2024-20076
CVE-2024-34726 CVE-2024-34725 CVE-2024-34724 CVE-2024-31335 CVE-2024-31334 CVE-2024-4610
CVE-2024-0153 CVE-2024-34721 CVE-2024-31331 CVE-2024-31339 CVE-2024-34722 CVE-2024-31332
CVE-2024-34723 CVE-2024-34720 CVE-2024-31320

LEGGI DI PIÙ →

17 SETTEMBRE 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 →

17 SETTEMBRE 2024

Sanata vulnerabilità in Apache OFBiz

(AL02/240805/CSIRT-ITA) - Aggiornamento

Apache Software Foundation ha rilasciato un aggiornamento di sicurezza per il prodotto OFBiz che sana una vulnerabilità con gravità "alta". Tale vulnerabilità, qualora sfruttata, potrebbe consentire, in determinate condizioni, a un utente malintenzionato remoto di manipolare l'output dello schermo sull'istanza interessata.

CVE-2024-38856

LEGGI DI PIÙ →

17 SETTEMBRE 2024

Vulnerabilità in Progress WhatsUp Gold

(AL02/240821/CSIRT-ITA) - Aggiornamento

Rilevate 3 vulnerabilità di sicurezza, di cui 2 con gravità "critica", nel prodotto WhatsUp Gold di Progress, software per il monitoraggio di infrastrutture IT.

CVE-2024-6670 CVE-2024-6671 CVE-2024-6672

LEGGI DI PIÙ →

17 SETTEMBRE 2024

Aggiornamenti Mensili Microsoft

(AL01/240911/CSIRT-ITA) - Aggiornamento

Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 79 nuove vulnerabilità, di cui 4 di tipo 0-day.

CVE-2024-38014	CVE-2024-38217	CVE-2024-38226	CVE-2024-43491	CVE-2024-43463	CVE-2024-43454
CVE-2024-43479	CVE-2024-30073	CVE-2024-26191	CVE-2024-43465	CVE-2024-21416	CVE-2024-38249
CVE-2024-43492	CVE-2024-38240	CVE-2024-38258	CVE-2024-38230	CVE-2024-37337	CVE-2024-37980
CVE-2024-43474	CVE-2024-38225	CVE-2024-38248	CVE-2024-38245	CVE-2024-38260	CVE-2024-43495
CVE-2024-26186	CVE-2024-38234	CVE-2024-43455	CVE-2024-43464	CVE-2024-38242	CVE-2024-43476
CVE-2024-38216	CVE-2024-43467	CVE-2024-43470	CVE-2024-38018	CVE-2024-43458	CVE-2024-38046
CVE-2024-43482	CVE-2024-37341	CVE-2024-43461	CVE-2024-37340	CVE-2024-37342	CVE-2024-43457
CVE-2024-38246	CVE-2024-43469	CVE-2024-38238	CVE-2024-38228	CVE-2024-37966	CVE-2024-38250
CVE-2024-38194	CVE-2024-38254	CVE-2024-37965	CVE-2024-38263	CVE-2024-37339	CVE-2024-38256
CVE-2024-38188	CVE-2024-38220	CVE-2024-38119	CVE-2024-38233	CVE-2024-38244	CVE-2024-38045
CVE-2024-38239	CVE-2024-38232	CVE-2024-38236	CVE-2024-43466	CVE-2024-38241	CVE-2024-38235
CVE-2024-37335	CVE-2024-38237	CVE-2024-38257	CVE-2024-38259	CVE-2024-38253	CVE-2024-43475
CVE-2024-38252	CVE-2024-37338	CVE-2024-38247	CVE-2024-38243	CVE-2024-43487	CVE-2024-38227
CVE-2024-38231					

LEGGI DI PIÙ →

17 SETTEMBRE 2024

Aggiornamenti di sicurezza Apple

(AL01/240917/CSIRT-ITA)

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

CVE-2024-40840	CVE-2024-40830	CVE-2024-44171	CVE-2024-40852	CVE-2024-27874	CVE-2024-27876
CVE-2024-27869	CVE-2024-44124	CVE-2024-44131	CVE-2024-40850	CVE-2024-27880	CVE-2024-44176
CVE-2024-44169	CVE-2024-44165	CVE-2024-44191	CVE-2024-44198	CVE-2024-40791	CVE-2024-44183
CVE-2023-5841	CVE-2024-44147	CVE-2024-44167	CVE-2024-40826	CVE-2024-44202	CVE-2024-44127
CVE-2024-40863	CVE-2024-44139	CVE-2024-44180	CVE-2024-44170	CVE-2024-44184	CVE-2024-27879
CVE-2024-40857	CVE-2024-44187	CVE-2024-40856	CVE-2024-44129	CVE-2024-44153	CVE-2024-44188
CVE-2024-40825	CVE-2024-44130	CVE-2024-44182	CVE-2024-44154	CVE-2024-40845	CVE-2024-40846
CVE-2024-44164	CVE-2024-40837	CVE-2024-40847	CVE-2024-40848	CVE-2024-44168	CVE-2024-27860
CVE-2024-27861	CVE-2024-40841	CVE-2024-27795	CVE-2024-44135	CVE-2024-44132	CVE-2024-44128
CVE-2024-44151	CVE-2024-27875	CVE-2024-44146	CVE-2023-4504	CVE-2024-44148	CVE-2024-44177
CVE-2024-40831	CVE-2024-40861	CVE-2024-44160	CVE-2024-44161	CVE-2024-44181	CVE-2024-27858
CVE-2024-40838	CVE-2024-44186	CVE-2024-39894	CVE-2024-44178	CVE-2024-44149	CVE-2024-40797
CVE-2024-44125	CVE-2024-44163	CVE-2024-40801	CVE-2024-44158	CVE-2024-40844	CVE-2024-40860
CVE-2024-44152	CVE-2024-44166	CVE-2024-44190	CVE-2024-44133	CVE-2024-40859	CVE-2024-41957
CVE-2024-40866	CVE-2024-40770	CVE-2024-23237	CVE-2024-44134	CVE-2024-44189	CVE-2024-40842
CVE-2024-40843	CVE-2024-40790	CVE-2024-44162	CVE-2024-40862	CVE-2024-27886	CVE-2024-40814

LEGGI DI PIÙ →

16 SETTEMBRE 2024

Vulnerabilità in prodotti Solarwinds

(AL03/240916/CSIRT-ITA)

Risolte 2 vulnerabilità di sicurezza, di cui una con gravità "critica" in SolarWinds Access Rights Manager (ARM), software utilizzato per la gestione e l'audit dei diritti di accesso degli utenti ai sistemi, ai dati e ai file. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto l'esecuzione di codice arbitrario sui dispositivi target.

CVE-2024-28991

LEGGI DI PIÙ →

16 SETTEMBRE 2024

Vulnerabilità in prodotti D-Link

(AL02/240916/CSIRT-ITA)

Rilevate 5 nuove vulnerabilità di sicurezza, di cui tre con gravità "critica", che interessano alcuni modelli di router wifi D-Link. Tali vulnerabilità potrebbero permettere ad un utente malevolo la possibilità di eseguire codice arbitrario sui dispositivi target, anche mediante credenziali codificate all'interno del software.

CVE-2024-45694 CVE-2024-45695 CVE-2024-45697 CVE-2024-45698 CVE-2024-45696

LEGGI DI PIÙ →

16 SETTEMBRE 2024

Ivanti: rilevato sfruttamento in rete della CVE-2024-8190 relativa al prodotto Cloud Service Appliance

(AL01/240916/CSIRT-ITA)

Rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-8190 – già sanata dal vendor – che interessa la soluzione Cloud Service Appliance (CSA) di Ivanti, appliance di rete per la gestione e la protezione dei dispositivi aziendali connessi a Internet.

CVE-2024-8190

LEGGI DI PIÙ →