Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

15 January 2024

Vulnerabilities

CISA has issued a warning about attackers actively exploiting a critical Microsoft SharePoint privilege escalation vulnerability

Tech-Wreck InfoSec Blog - January 13 2024

CISA has issued a warning about attackers actively exploiting a critical Microsoft SharePoint privilege escalation vulnerability, tracked as CVE-2023-29357, which allows remote attackers to gain admin privileges on unpatched servers by using spoofed JWT authentication tokens.

US, others potentially targeted by new Volt Typhoon attacks exploiting Cisco router bugs

SC Magazine US - January 12 2024

The U.S., Australia, India, and the UK are having their government institutions subjected to new attacks by Chinese advanced persistent threat operation Volt Typhoon leveraging a pair of critical vulnerabilities in end-of-life Cisco small business RV320/325 VPN routers, tracked as CVE-2019-1652 and CVE-2019-1653, according to SecurityWeek.

Juniper Networks fixed a critical RCE bug in its firewalls and switches

Security Affairs - January 12 2024

Juniper Networks fixed a critical pre-auth remote code execution (RCE) flaw, tracked as CVE-2024-21591, in its SRX Series firewalls and EX Series switches. Juniper Networks released security updates to address a critical pre-auth remote code execution (RCE) vulnerability, tracked as CVE-2024-21591, that resides in SRX Series firewalls and EX Series switches.

Siemens Teamcenter Visualization and JT2Go

CISA Current Activity - January 11 2024

EXECUTIVE SUMMARY CVSS v3: 7.8 ATTENTION: Low attack complexity Vendor: Siemens Equipment: JT2Go, Teamcenter Visualization Vulnerabilities: Out-of-bounds Read, NULL Pointer Dereference, Stack-based Buffer Overflow 2. RISK EVALUATION Successful exploitation of these vulnerabilities could allow an attacker to execute code in the context of the software's current process or crash the application causing a denial of service.

Siemens SICAM A8000

CISA Current Activity - January 11 2024

EXECUTIVE SUMMARY CVSS v3 6.6 ATTENTION: Exploitable remotely Vendor: Siemens Equipment: SICAM A8000 Vulnerability: Use of Uninitialized Resource 2. RISK EVALUATION Successful exploitation of this vulnerability could allow an authenticated remote attacker to inject commands that are executed on the device with root privileges during device startup.

Siemens SIMATIC CN 4100

CISA Current Activity - January 11 2024

EXECUTIVE SUMMARY CVSS v3 9.8 ATTENTION: Exploitable remotely/low attack complexity Vendor: Siemens Equipment: SIMATIC CN 4100 Vulnerabilities: Authorization Bypass Through User-Controlled Key, Improper Input Validation, Use of Default Credentials 2. RISK EVALUATION Successful exploitation of these vulnerabilities could allow an attacker to remotely login as root or cause denial of service condition of the device.

GitLab Releases Updates to Address Critical Vulnerabilities

Dark Reading - January 12 2024

In a newly released update, GitLab reports that it is releasing versions 16.7.2, 16.6.3, and 16.5.6 for GitLab Community Edition (CE) as well as Enterprise Edition (EE) in order to address a series of critical vulnerabilities. Two critical vulnerabilities, alongside one each for high, medium, and low, are listed as part of the fixes that the vendor is urgently recommending as soon as possible.

UK cyber

Human Error and Insiders Expose Millions in UK Law Firm Data Breaches

Infosecurity Today - January 12 2024

UK law firms are falling victim to data breaches primarily because of insiders and human error, according to an analysis of data from the the Information Commissioner’s Office (ICO).

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Medusa group steps up ransomware activities

CSO Magazine - January 12 2024

Medusa uses initial access brokers for network access. Other distinctions include Medusa having its own media and branding team, focusing on exploiting internet-facing vulnerabilities, and using initial access brokers (IABs) to gain access to systems.

Akira ransomware targets Finnish organizations

Security Affairs - January 13 2024

The Finish National Cybersecurity Center (NCSC-FI) warns of increased Akira ransomware attacks targeting NAS and tape backup devices of organizations in the country. The Finish National Cybersecurity Center (NCSC-FI) reported an increase in Akira ransomware attacks, targeting organizations in the country.

New Findings Challenge Attribution in Denmark's Energy Sector Cyberattacks

The Hacker News - January 14 2024

The cyber attacks targeting the energy sector in Denmark last year may not have had the involvement of the Russia-linked Sandworm hacking group, new findings from Forescout show.