Scottish
Cyber
Coordination
Centre

Daily threat bulletin

23 September 2024

Vulnerabilities

Critical Ivanti Cloud Appliance Vulnerability Exploited in Active Cyberattacks

The Hacker News - 20 September 2024 10:48

Ivanti has revealed that a critical security flaw impacting Cloud Service Appliance (CSA) has come under active exploitation in the wild. The new vulnerability, assigned the CVE identifier CVE-2024-8963, carries a CVSS score of 9.4 out of a maximum of 10.0.

Configuration flaw puts ServiceNow Knowledge Base articles at risk

Security Magazine - 20 September 2024 13:00

More than 1,000 ServiceNow Knowledge Base articles were found to be misconfigured.

Zero-Click MediaTek Bug Opens Phones, Wi-Fi to Takeover

darkreading - 20 September 2024 19:08

Critical-rated CVE-2024-20017 allows remote code execution (RCE) on a range of phones and Wi-Fi access points from a variety of OEMs.

Patch this Critical Safeguard for Privileged Passwords Authentication Bypass Flaw

Cyware News - Latest Cyber News - 21 September 2024 01:00

Researchers have released technical details about CVE-2024-45488, a critical authentication bypass vulnerability affecting One Identity’s Safeguard for Privileged Passwords (SPP), which could allow attackers to gain full administrative access.

Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-45229

CISA Advisories -

Versa Networks has released an advisory for a vulnerability (CVE-2024-45229) affecting Versa Director. A cyber threat actor could exploit this vulnerability to exercise unauthorized REST APIs. CISA urges organizations to apply necessary updates, hunt for any malicious activity, report any positive findings to CISA, and review the following for more information.

Threat actors and malware

OP KAERB: Europol dismantled phishing scheme targeting mobile users

Security Affairs - 21 September 2024 14:51

A joint international law enforcement operation led by Europol dismantled a major phishing scheme targeting mobile users. Europol supported European and Latin American law enforcement agencies in dismantling an international criminal network that unlocks stolen or lost mobile phones using a phishing platform.

New PondRAT Malware Hidden in Python Packages Targets Software Developers

The Hacker News - 23 September 2024 13:09

Threat actors with ties to North Korea have been observed using poisoned Python packages as a way to deliver a new malware called PondRAT as part of an ongoing campaign. PondRAT, according to new findings from Palo Alto Networks Unit 42, is assessed to be a lighter version of POOLRAT (aka SIMPLESEA), a known macOS backdoor that has been previously attributed to the Lazarus Group.

Chinese Hackers Exploit GeoServer Flaw to Target APAC Nations with EAGLEDOOR Malware

The Hacker News - 23 September 2024 11:19

A suspected advanced persistent threat (APT) originating from China targeted a government organization in Taiwan, and possibly other countries in the Asia-Pacific (APAC) region, by exploiting a recently patched critical security flaw impacting OSGeo GeoServer GeoTools.