Scottish
Cyber
Coordination
Centre

Daily threat bulletin

3 July 2024

Vulnerabilities

PTC License Server Bug Needs Immediate Patch Against Critical Flaw

darkreading - 02 July 2024 19:42

Creo Elements/Direct License Servers, which enable industrial design and modeling software, are exposed to the Internet, leaving critical infrastructure vulnerable to remote code execution.

Google Patches 25 Android Flaws, Including Critical Privilege Escalation Bug

SecurityWeek - 02 July 2024 15:18

Google ships an Android security update with fixes for 15 vulnerabilities, including a critical-severity flaw in Framework.The post Google Patches 25 Android Flaws, Including Critical Privilege Escalation Bug appeared first on SecurityWeek.

Splunk Patches High-Severity Vulnerabilities in Enterprise Product

SecurityWeek - 02 July 2024 13:22

Splunk has patched multiple vulnerabilities in Splunk Enterprise, including high-severity remote code execution bugs.The post Splunk Patches High-Severity Vulnerabilities in Enterprise Product appeared first on SecurityWeek.

Patch Now: Cisco Zero-Day Under Fire From Chinese APT

darkreading - 02 July 2024 14:18

Threat actor "Velvet Ant" has been exploiting a vulnerability in Cisco's NX-OS Software for managing a variety of switches, executing commands and dropping custom malware.

Threat actors and malware

South Korean ERP Vendor's Server Hacked to Spread Xctdoor Malware

The Hacker News - 03 July 2024 10:03

An unnamed South Korean enterprise resource planning (ERP) vendor's product update server has been found to be compromised to deliver a Go-based backdoor dubbed Xctdoor.The AhnLab Security Intelligence Center (ASEC), which identified the attack in May 2024, did not attribute it to a known threat actor or group, but noted that the tactics overlap with that of Andariel, a sub-cluster within the

How MFA Failures are Fueling a 500% Surge in Ransomware Losses

The Hacker News - 02 July 2024 17:30

The cybersecurity threat landscape has witnessed a dramatic and alarming rise in the average ransomware payment, an increase exceeding 500%. Sophos, a global leader in cybersecurity, revealed in its annual “State of Ransomware 2024” report that the average ransom payment has increased 500% in the last year with organizations that paid a ransom reporting an average payment of $2 million, up from