Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

5 March 2024

Vulnerabilities

ScreenConnect flaws exploited to drop new ToddleShark malware
BleepingComputer.com - March 4 2024

The North Korean APT hacking group Kimsuky is exploiting ScreenConnect flaws, particularly CVE-2024-1708 and CVE-2024-1709, to infect targets with a new malware variant dubbed ToddleShark.

dnf5daemon-server: Local root Exploit and Local Denial-of-Service in dnf5 D-Bus Components (CVE-2024-1929, CVE-2024-1930)
Open Source Security - March 4 2024

Posted by Matthias Gerstner on Mar 04Hello list,

please find below a report about a local root exploit and other issues
in dnf5daemon-server. We also offer a rendered HTML version of the
report on our blog.

Django: CVE-2024-27351: Potential regular expression denial-of-service in django[.]utils[.]text[.]Truncator[.]words()
Open Source Security - March 4 2024

Posted by Mariusz Felisiak on Mar
04hxxps://www[.]djangoproject[.]com/weblog/2024/mar/04/security-releases/

Critical vulnerabilities in TeamCity JetBrains fixed, release of technical details imminent, patch quickly! (CVE-2024-27198, CVE-2024-27199)
Help Net Security - March 4 2024

JetBrains has fixed two critical security vulnerabilities (CVE-2024-27198, CVE-2024-27199) affecting TeamCity On-Premises and is urging customers to patch them immediately. “Rapid7 originally identified and reported these vulnerabilities to us and has...

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[Response to CISA Advisory (AA24-060B): Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways]
Security Boulevard - RSS - March 4 2024

In response to the recently published CISA Advisory (AA24-060B) that disseminates observed threat actor activities, Indicators of Compromise (IOCs), and mitigations associated with ongoing incident response activities in connection with the recent Ivanti...

Malware and threat actors

[Hacktivist Collective NoName057(16) Strikes European Targets]
Infosecurity Today - March 4 2024

Sekoia[.]io observed developments in the group's DDoS tools, including updates enhancing compatibility with different processor architectures and OS

[TA577 Exploits NTLM Authentication Vulnerability]
Infosecurity Today - March 4 2024

Proofpoint warned the method could be used for data gathering and further malicious activities

[New GTPDOOR backdoor is designed to target telecom carrier networks]
Security Affairs - March 4 2024

Researcher HaxRob discovered a previously undetected Linux backdoor named GTPDOOR, designed to target telecom carrier networks. Security researcher HaxRob discovered a previously undetected Linux backdoor dubbed GTPDOOR, which is specifically crafted to carry out stealth cyber operations within mobile carrier networks. I recently found two very interesting Linux binaries uploaded to Virustotal.

[Predator Spyware Alive & Well and Expanding]
Dark Reading - March 4 2024

The infamous Predator mobile spyware operation publicly exposed in an eye-popping report last year by Amnesty International has revamped its malware delivery network and expanded its reach into Botswana and the Philippines. Researchers from Recorded Future's Insikt Group, which spotted Predator's updated architecture, said the mercenary

mobile spyware enterprise now operates in at least 11 countries with the addition of Botswana and the Philippines.