Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

2 February 2024

Vulnerabilities

Ivanti Releases Zero-Day Patches and Reveals Two New Bugs

Infosecurity Today - February 1 2024

Ivanti has finally released updates to fix two zero-day bugs and two new high-severity vulnerabilities

New Windows Event Log zero-day flaw gets unofficial patches

BleepingComputer.com - February 1 2024

Free unofficial patches are available for a new Windows zero-day vulnerability dubbed 'EventLogCrasher' that lets attackers remotely crash the Event Log service on devices within the same Windows domain.

FritzFrog botnet is exploiting Log4Shell bug now, experts say

Record by Recorded Future - February 1 2024

A variant of a long-running botnet is now abusing the Log4Shell vulnerability but is going beyond internet-facing applications and is targeting all hosts in a victim's internal network. Researchers at Akamai explain the shift in the FritzFrog botnet.

Moby and Open Container Initiative Release Critical Updates for Multiple Vulnerabilities Affecting Docker-related Components

CISA Current Activity - February 1 2024

Moby and the Open Container Initiative (OCI) have released updates for multiple vulnerabilities (CVE-2024-23651, CVE-2024-23652, CVE-2024-23653, CVE-2024-21626) affecting Docker-related components, including Moby BuildKit and OCI runc. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.

Malware and threat actors

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[Feds Confirm Remote Killing of Volt Typhoon's SOHO Botnet]

Dark Reading - February 1 2024

US law enforcement has disrupted the infrastructure of the notorious China-sponsored cyberattack group known as Volt Typhoon. The advanced persistent threat (APT), which FBI Director Christopher Wray said this week is "the defining cyber-threat of this era," is known for managing a sprawling botnet created by compromising poorly protected small office/home office (SOHO) routers. The state-backed group uses it as a launchpad for other attacks, particularly on US critical infrastructure, because the botnet's distributed nature makes the activity hard to trace.

[Multiple malware used in attacks exploiting Ivanti VPN flaws]

Security Affairs - February 1 2024

Mandiant spotted new malware used by a China-linked threat actor UNC5221 targeting Ivanti Connect Secure VPN and Policy Secure devices. Mandiant researchers discovered new malware employed by a China-linked APT group known as UNC5221 and other threat groups targeting Ivanti Connect Secure VPN and Policy Secure devices.

[PurpleFox malware infects thousands of computers in Ukraine]

Bleeping Computer - February 1 2024

The Computer Emergency Response Team in Ukraine (CERT-UA) is warning about a PurpleFox malware campaign that has infected at least 2,000 computers in the country. The exact impact of this widespread infection and whether it has affected state organizations or regular people's computers hasn't been determined, but the agency has shared detailed information on how to locate infections and remove the malware.