Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

4 March 2024

Vulnerabilities

CISA warns of Microsoft Streaming bug exploited in malware attacks
Bleeping Computer - March 1 2024

CISA ordered U.S. Federal Civilian Executive Branch (FCEB) agencies to secure their Windows systems against a high-severity vulnerability in the Microsoft Streaming Service (MSKSSRV[.]SYS) that's actively exploited in attacks. The security flaw (tracked as **CVE-2023-29360**) is due to an untrusted pointer dereference weakness that enables local attackers to gain SYSTEM privileges in low-complexity attacks that don't require user interaction.

Windows Kernel bug fixed last month exploited as zero-day since August
Bleeping Computer - March 2 2024

Microsoft patched a high-severity Windows Kernel privilege escalation vulnerability in February, six months after being informed that the flaw was being exploited as a zero-day. Tracked as **CVE-2024-21338**, the security flaw was found by Avast Senior Malware Researcher Jan Vojtěšek in the appid[.]sys Windows AppLocker driver and reported to Microsoft last August as an actively exploited zero-day. The vulnerability impacts systems running multiple versions of Windows 10 and Windows 11 (including the latest releases), as well as Windows Server 2019 and 2022.

Azure-connected IoT devices at risk of RCE due to critical vulnerability
SC Magazine US - February 29 2024

Internet-of-things (IoT) devices that use Microsoft's uAMQP C library for communication with Azure Cloud Services may be vulnerable to remote code execution (RCE) due to a critical vulnerability disclosed on Tuesday. The Advanced Message Queuing Protocol (AMQP) is used by Azure Cloud Services, including Azure Service Bus, Azure Event Hubs and Azure IoT Hubs, for communication between various devices and applications across the cloud environment.

CISA cautions against using hacked Ivanti VPN gateways even after factory resets
Bleeping Computer - February 29 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) revealed today that attackers who hack Ivanti VPN appliances using one of multiple actively exploited vulnerabilities may be able to maintain root persistence even after performing factory resets. Furthermore, they can also evade detection by Ivanti's internal and external Integrity Checker Tool (ICT) on Ivanti Connect Secure and Policy Secure gateways compromised using **CVE-2023-46805, CVE-2024-21887, CVE-2024-22024, and CVE-2024-21893 exploits.**

WordPress LiteSpeed Cache Plugin Cross Site Scripting (XSS) Vulnerability (CVE-2023-40000)

Qualys Threat Protection - February 29 2024

WordPress LiteSpeed Cache plugin is vulnerable to cross-site scripting vulnerability that may lead to privilege escalation. **CVE-2023-40000** may allow an unauthenticated user to steal sensitive information and elevate their privilege on the WordPress.

Malware and threat actors

Lazarus Group observed exploiting an admin-to-kernel Windows zero-day

SC Media - March 1 2024

Avast researchers say North Korean APT has developed a new, stealthier rootkit and appears poised to continue enhancements.

Hackers target FCC, crypto firms in advanced Okta phishing attacks

Bleeping Computer - March 2 2024

A new phishing kit named CryptoChameleon is being used to target Federal Communications Commission (FCC) employees, using specially crafted single sign-on (SSO) pages for Okta that appear remarkably similar to the originals. The same campaign also targets users and employees of cryptocurrency platforms, such as Binance, Coinbase, Kraken, and Gemini, using phishing pages that impersonate Okta, Gmail, iCloud, Outlook, Twitter, Yahoo, and AOL.

Stealthy GTPDOOR Linux malware targets mobile operator networks

Bleeping Computer - March 3 2024

Security researcher HaxRob discovered a previously unknown Linux backdoor named GTPDOOR, designed for covert operations within mobile carrier networks. The threat actors behind GTPDOOR are believed to target systems adjacent to the GPRS roaming

eXchange (GRX), such as SGSN, GGSN, and P-GW, which can provide the attackers direct access to a telecom's core network. The GRX is a component of mobile telecommunications that facilitates data roaming services across different geographical areas and networks.

NoName Ransomware Claims Cyberattack on Denmark's Key Websites

The Cyber Express - March 4 2024

The NoName ransomware group has claimed responsibility for targeting multiple websites in Denmark, including prominent entities such as Movia, Din Offentlige Transport, the Ministry of Transport, Copenhagen Airports, and Danish Shipping.

FBI, CISA Release IoCs for Phobos Ransomware

Dark Reading - February 29 2024

The FBI and the US Cybersecurity and Infrastructure Security Agency (CISA) have released details on the tactics and techniques threat actors are using to deploy the Phobos ransomware strain on target networks.

New SPIKEDWINE APT group is targeting officials in Europe

Security Affairs - February 29 2024

A new threat actor, tracked as dubbed SPIKEDWINE, has been observed targeting officials in Europe with a previously undetected backdoor WINELOADER.