Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

1 March 2024

Vulnerabilities

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

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.

Delta Electronics CNCSoft-B
CISA Current Activity - February 29 2024

Vendor: Delta Electronics Equipment: CNCSoft-B Vulnerability: Stack-based Buffer Overflow. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code.

Lazarus Hackers Exploited Windows Kernel Flaw as Zero-Day in Recent Attacks
The Hacker News - February 29 2024

The notorious Lazarus Group actors exploited a recently patched privilege escalation flaw in the Windows Kernel as a zero-day to obtain kernel-level access and disable security software on compromised hosts. The

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

vulnerability in question is CVE-2024-21338 (CVSS score: 7.8), which can permit an attacker to gain SYSTEM privileges.

Malware and threat actors

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.