Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

31 January 2024

Vulnerabilities

Ivanti Avalanche Directory Traversal Vulnerability (CVE-2023-41474)

Qualys Threat Protection - January 30 2024

Ivanti Avalanche, a popular mobile device management system, is vulnerable to a limited unauthenticated path traversal vulnerability, tracked as CVE-2023-41474.

Active Exploitation of Atlassian Confluence RCE Vulnerability (CVE-2023-22527)

Cyble Blog - January 30 2024

Cyble's Global Sensor Intelligence (CGSI) network picks up scanning attempts aiming to exploit a recent Vulnerability in Atlassian Confluence.

Ivanti Zero-Day Patches Delayed as 'KrustyLoader' Attacks Mount

Dark Reading - January 30 2024

The RCE/auth bypass bugs in Connect Secure VPNs have gone unpatched for 20 days as state-sponsored groups continue to backdoor Ivanti gear.

Malware and threat actors

New ZLoader Malware Variant Surfaces with 64-bit Windows Compatibility

The Hacker News - January 30 2024

Threat hunters have identified a new campaign that delivers the ZLoader malware, resurfacing nearly two years after the botnet's infrastructure was dismantled in April 2022. A new variant of the malware is said to have been in development since September 2023, Zscaler ThreatLabz said in an analysis published this month.

Microsoft Teams phishing pushes DarkGate malware via group chats

Bleeping Computer - January 30 2024

TLP CLEAR: Disclosure is not limited

New phishing attacks abuse Microsoft Teams group chat requests to push malicious attachments that install DarkGate malware payloads on victims' systems. The attackers used what looks like a compromised Teams user (or domain) to send over 1,000 malicious Teams group chat invites, according to AT&T Cybersecurity research. After the targets accept the chat request, the threat actors trick them into downloading a file using a double extension named 'Navigating Future Changes October 2023[.]pdf[.]msi,' a common DarkGate tactic.

Rust Payloads Exploiting Ivanti 0-Days Linked to Sliver Toolkit

Infosecurity Today - January 30 2024

After analyzing the Rust payloads exploiting Ivanti ConnectSecure vulnerabilities, Synacktiv found they all enabled a post-exploitation toolkit.