Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

1 February 2024

Vulnerabilities

Ivanti Discloses Additional Zero-Day That Is Being Exploited

DataBreachToday.eu - January 31 2024

Company Starts Patch Rollout for Flaws Exploited by Likely Chinese Intelligence Op Corporate VPN maker Ivanti on Wednesday began a belated patch rollout for zero-day flaws that many cybersecurity firms say paved the way for an espionage hacking operation.

CISA Warns of Active Exploitation of Critical Vulnerability in iOS, iPadOS, and macOS

The Hacker News - February 1 2024

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a high-severity flaw impacting iOS, iPadOS, macOS, tvOS, and watchOS to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. The vulnerability, tracked as CVE-2022-48618 (CVSS score: 7.8), concerns a bug in the kernel component.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Current Activity - January 31 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2022-48618 - Apple Multiple Products Improper Authentication Vulnerability.

CISA and FBI Release Secure by Design Alert Urging Manufacturers to Eliminate Defects in SOHO Routers

CISA Current Activity - January 31 2024

Today, CISA and the Federal Bureau of Investigation (FBI) published guidance on Security Design Improvements for SOHO Device Manufacturers as a part of the new Secure by Design (SbD) Alert series that focuses on how manufacturers should shift the burden of security away from customers by integrating security into product design and development.

TLP CLEAR: Disclosure is not limited

A zero-day vulnerability (and PoC) to blind defenses relying on Windows event logs

Help Net Security - January 31 2024

A zero-day vulnerability that, when triggered, could crash the Windows Event Log service on all supported (and some legacy) versions of Windows could spell trouble for enterprise defenders.

Relution Remote Code Execution via Java Deserialization Vulnerability

Praetorian - February 1 2024

Overview In this article we discuss a recent deserialization vulnerability we found in Relution (CVE-2023-48178), a mobile device management product that is popular among multinational German corporations. CVE-2023-48178 can potentially lead to remote code...

Hitron DVR Zero-Day Vulnerabilities Exploited by InfectedSlurs Botnet

SecurityWeek RSS Feed - January 31 2024

Akamai flags six zero-day vulnerabilities in Hitron DVRs exploited to ensnare devices in the InfectedSlurs botnet. The post Hitron DVR Zero-Day Vulnerabilities Exploited by InfectedSlurs Botnet appeared first on SecurityWeek.

Malware and threat actors

DarkGate Malware: Attackers Send Over 1,000 Microsoft Teams Group Chats Invites to Infect Systems

Tech Times - January 31 2024

In a recent surge of cyber threats, attackers are exploiting Microsoft Teams, a widely used collaboration platform. The attackers employ phishing tactics, leveraging compromised Teams accounts to send over 1,000 malicious group chat invites.

Nearly 4-year-old Cisco vuln linked to recent Akira ransomware attacks

The Register - Security - January 31 2024

Evidence mounts of an exploit gatekept within Russia's borders Security researchers believe the Akira ransomware group could be exploiting a nearly four-year-old Cisco vulnerability and using it as an entry point into organizations' systems.

Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Threat actors exploit Ivanti VPN bugs to deploy KrustyLoader Malware

Security Affairs - January 31 2024

Threat actors are exploiting recently disclosed zero-day flaws in Ivanti Connect Secure (ICS) VPN devices to deliver KrustyLoader. In early January 2024, software firm Ivanti reported that threat actors were exploiting two zero-day vulnerabilities (CVE-2023-46805, CVE-2024-21887) in Connect Secure (ICS) and Policy Secure to remotely execute arbitrary commands on targeted gateways.