Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

17 January 2024

Vulnerabilities

Citrix warns of new Netscaler zero-days exploited in attacks
BleepingComputer.com - January 16 2024

Citrix urged customers on Tuesday to immediately patch Netscaler ADC and Gateway appliances exposed online against two actively exploited zero-day vulnerabilities.

Atlassian fixed critical RCE in older Confluence versions
Security Affairs - January 16 2024

Atlassian warns of a critical remote code execution issue in Confluence Data Center and Confluence Server that impacts older versions. Atlassian warns of a critical remote code execution vulnerability, tracked as CVE-2023-22527 (CVSS score 10.0), in Confluence Data Center and Confluence Server that impacts older versions.

Ivanti Zero-Day Exploits Skyrocket Worldwide; No Patches Yet
Dark Reading - January 16 2024

Anyone who hasn't mitigated two zero-day security bugs in Ivanti VPNs may already be compromised by a Chinese nation-state actor.

VMware fixed a critical flaw in Aria Automation. Patch it now!
Security Affairs - January 16 2024

VMware warns customers of a critical vulnerability impacting its Aria Automation multi-cloud infrastructure automation platform. VMware Aria Automation (formerly vRealize Automation) is a modern cloud automation platform that simplifies and streamlines the deployment, management, and governance of cloud infrastructure and applications.

CISA Adds One Known Exploited Vulnerability to Catalog
CISA Current Activity - January 16 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2018-15133 Laravel Deserialization of

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Untrusted Data Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

178K+ SonicWall Firewalls Vulnerable to DoS, RCE Attacks

Dark Reading - January 16 2024

Two unauthenticated denial-of-service (DoS) vulnerabilities are threatening the security of SonicWall next-generation firewall devices, exposing more than 178,000 of them to both DoS as well as remote code execution (RCE) attacks.

Google fixes first actively exploited Chrome zero-day of 2024

BleepingComputer.com - January 16 2024

Google has released security updates to fix the first Chrome zero-day vulnerability exploited in the wild since the start of the year.

CISA Releases Two Industrial Control Systems Advisories

CISA Current Activity - January 16 2024

CISA released two Industrial Control Systems (ICS) advisories on January 16, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. ICSA-24-016-01 SEW-EURODRIVE MOVITOOLS MotionStudio ICSA-24-016-02 Integration Objects OPC UA Server Toolkit.

Ransomware

Ransomware gang demands €10 million after attacking Spanish council

Record by Recorded Future - January 16 2024

The mayor of Calvià, a municipality on the Spanish island of Majorca, has said the city council will not be paying an approximately €10 million extortion fee demanded by criminals following a ransomware attack. Calvià, a region on the southwestern part of...

Malware and threat actors

Detailed Analysis of DarkGate; Investigating new top-trend backdoor malware

S2W Blog - January 16 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

DarkGate is a malware that has been developed since 2017 and sold as Malware-as-a-Service.DarkGate was not widely used until 2021.

CISA and FBI Release Known IOCs Associated with Androxgh0st Malware

CISA Current Activity - January 16 2024

Today, CISA and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), Known Indicators of Compromise Associated with Androxgh0st Malware, to disseminate known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with threat actors deploying Androxgh0st malware.