TLP CLEAR: Disclosure is not limited

Daily threat summary

15 March 2024

Vulnerabilities

PaperCut NG/MF Security Bulletin

NCSC-FI Daily Vulnerabilities - March 15 2024

Multiple security vulnerabilities have been addressed in the latest PaperCut NG/MF version release. The most serious vulnerability has been rated as high severity. This high severity vulnerability could allow an attacker to use maliciously formed API requests to gain access to an API authorization level with elevated privileges.

Cisco fixed high-severity elevation of privilege and DoS bugs

Security Affairs - March 14 2024

Cisco this week addressed high-severity elevation of privilege and denial-of-service (DoS) vulnerabilities in IOS RX software. Cisco addressed multiple vulnerabilities in IOS RX software, including three high-severity issues that can be exploited to elevate privileges and trigger a denial-of-service (DoS) condition.

Recent DarkGate campaign exploited Microsoft Windows zero-day

Security Affairs - March 14 2024

Researchers recently uncovered a DarkGate campaign in mid-January 2024, which exploited Microsoft zero-day vulnerability.

CVE-2023-48788: Critical Fortinet FortiClientEMS SQL Injection Vulnerability

Tenable Blog - March 14 2024

Fortinet warns of a critical SQL Injection vulnerability that could allow an unauthenticated attacker to execute arbitrary code on vulnerable FortiClientEMS software.

PoC for critical Arcserve UDP vulnerabilities published (CVE-2024-0799, CVE-2024-0800)

Help Net Security - News - March 14 2024

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Arcserve has fixed critical security vulnerabilities (CVE-2024-0799, CVE-2024-0800) in its Unified Data Protection (UDP) solution that can be chained to upload malicious files to the underlying Windows system.

Kubernetes Vulnerability Allows Remote Code Execution on Windows Endpoints

SecurityWeek RSS Feed - March 14 2024

A high-severity Kubernetes vulnerability tracked as CVE-2023-5528 can be exploited to execute arbitrary code on Windows endpoints. The post Kubernetes Vulnerability Allows Remote Code Execution on Windows Endpoints appeared first on SecurityWeek.

Malware and threat actors

Spinning Yarn Malware

Red Sky Alliance - X-Industry - RSS - March 14 2024

Linux Users Beware -- The Spinning YARN malware campaign targets misconfigured servers running Apache Hadoop YARN, Docker, Confluence, and Redis web-facing services. Cado Security Labs has discovered an emerging Linux malware campaign dubbed Spinning Yarn.

RedLine malware top credential stealer of last 6 months

SC Magazine US - March 14 2024

RedLine malware was used to steal more than 170 million passwords over the last six months, which makes it the most notorious credential stealer during that time, according to research published March 12.

RedCurl Cybercrime Group Abuses Windows PCA Tool for Corporate Espionage

The Hacker News - March 14 2024

The Russian-speaking cybercrime group called RedCurl is leveraging a legitimate Microsoft Windows component called the Program Compatibility Assistant (PCA) to execute malicious commands.

Ande Loader Malware Targets Manufacturing Sector in North America

The Hacker News - March 14 2024

The threat actor known as Blind Eagle has been observed using a loader malware called Ande Loader to deliver remote access trojans (RATs) like Remcos RAT and NjRAT.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited