Scottish Cyber Coordination Centre

# Daily threat bulletin

21 May 2024

## Vulnerabilities

### Critical Fluent Bit flaw impacts all major cloud providers

BleepingComputer - 20 May 2024 18:12

A critical Fluent Bit vulnerability that can be exploited in denial-of-service and remote code execution attacks impacts all major cloud providers and many technology giants. [...]

### QNAP QTS zero-day in Share feature gets public RCE exploit

BleepingComputer - 20 May 2024 11:57

An extensive security audit of QNAP QTS, the operating system for the company's NAS products, has uncovered fifteen vulnerabilities of varying severity, with eleven remaining unfixed. [...]

### "Linguistic Lumberjack" Vulnerability Discovered in Popular Logging Utility Fluent Bit

The Hacker News - 21 May 2024 13:13

Cybersecurity researchers have discovered a critical security flaw in a popular logging and metrics utility called Fluent Bit that could be exploited to achieve denial-of-service (DoS), information disclosure, or remote code execution.

### CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-4947 - Google Chromium V8 Type Confusion Vulnerability and CVE-2023-43208 - NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability.

## Threat actors and malware

### GitCaught campaign relies on Github and Filezilla to deliver multiple malware

Security Affairs - 20 May 2024 15:20

Researchers discovered a sophisticated cybercriminal campaign by Russian-speaking threat actors that used GitHub to distribute malware. Recorded Future's Insikt Group discovered a sophisticated cybercriminal campaign by Russian-speaking threat actors from the Commonwealth of Independent States (CIS). The attackers, tracked as GitCaught, used a GitHub profile to impersonate legitimate software applications, including 1Password, Bartender 5, and [...]

Scottish Cyber Coordination Centre

## Iranian MOIS-Linked Hackers Behind Destructive Attacks on Albania and Israel

The Hacker News - 20 May 2024 22:35

An Iranian threat actor affiliated with the Ministry of Intelligence and Security (MOIS) has been attributed as behind destructive wiping attacks targeting Albania and Israel under the personas Homeland Justice and Karma, respectively.

## Foxit PDF Reader Flaw Exploited by Hackers to Deliver Diverse Malware Arsenal

The Hacker News - 20 May 2024 18:50

Multiple threat actors are weaponizing a design flaw in Foxit PDF Reader to deliver a variety of malware such as Agent Tesla, AsyncRAT, DCRat, NanoCore RAT, NjRAT, Pony, Remcos RAT, and XWorm."This exploit triggers security warnings that could deceive unsuspecting users into executing harmful commands," Check Point said in a technical report.

## GitCaught Campaign Leverages GitHub Repositories and Fake Profiles for Malicious Infrastructure

Cyware News - Latest Cyber News - 21 May 2024 01:00

Insikt Group uncovered a sophisticated campaign led by Russian-speaking actors who used GitHub profiles to spoof legitimate software apps and distribute various malware, including Atomic macOS Stealer (AMOS) and Vidar.