Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

# Daily threat summary

23 January 2024

## Vulnerabilities

### Godzilla Web Shell Attacks Stomp on Critical Apache ActiveMQ Flaw
Dark Reading - January 22 2024

Threat actors have unleashed a fresh wave of cyberattacks targeting a critical remote code-execution (RCE) vulnerability in Apache ActiveMQ, for which the Apache Software Foundation (ASF) issued a patch back in October. In many of the attacks, the adversary has been dropping a payload based on Godzilla, a known Web shell that enables them to squash compromised systems and gain complete control. The ActiveMQ vulnerability, tracked as CVE-2023-46604, carries a max-severity score of 10 out of 10 on the CVSS 3.0 scale, and affects multiple versions of the widely used open source message broker technology (including Apache ActiveMQ versions before 5.18.3; 5.17.6. and ActiveMQ Legacy OpenWire Module before 5.18.3 and before 5.17.6).

### CISA Adds One Known Exploited Vulnerability to Catalog
CISA Current Activity - January 22 2024

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-34048 VMware vCenter Server Out-of-Bounds Write Vulnerability.

### Apple Issues Patch for Critical Zero-Day in iPhones, Macs - Update Now
The Hacker News - January 23 2024

Apple on Monday released security updates for iOS, iPadOS, macOS, tvOS, and Safari web browser to address a zero-day flaw that has come under active exploitation in the wild. The issue, tracked as CVE-2024-23222, is a type confusion bug that could be exploited by a threat actor to achieve arbitrary code execution when processing maliciously crafted web content.

### Hackers start exploiting critical Atlassian Confluence RCE flaw
BleepingComputer.com - January 22 2024

Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

Security researchers are observing exploitation attempts for the CVE-2023-22527 remote code execution flaw vulnerability that affects outdated versions of Atlassian Confluence servers.

## Ransomware

### Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver

Trend Micro Simply Security - RSS - January 23 2024

In this blog, we detail our investigation of the Kasseika ransomware and the indicators we found suggesting that the actors behind it have acquired access to the source code of the notorious BlackMatter ransomware.

### Newly emergent 3AM ransomware operation's ties examined

SC Magazine US - January 23 2024

Attacks exploiting a critical out-of-bounds write zero-day vulnerability in VMware Center Server, tracked as CVE-2023-34048, have been deployed by Chinese cyberespionage operation UNC3886 since 2021, two years before the flaw was identified and addressed, reports The Hacker News.

## Malware and threat actors

### Widespread phishing campaign deployed by reemerging TA866

SC Magazine US - January 23 2024

Threat operation TA866 has reemerged with a new massive phishing campaign aimed at North America after being absent from the threat landscape for nine months, The Hacker News reports. Thousands of fraudulent invoice emails that included PDF attachments with malicious OneDrive URLs were leveraged by attackers to facilitate the distribution of a WasabiSeed and Screenshotter malware variant, according to a Proofpoint report.

### Midnight Blizzard attack highlights worrying flaws in Microsoft security

MalwareTips.com - January 22 2024

Midnight blizzard exfiltrated some emails and attached documents, apparently targeting email accounts for “information related to Midnight Blizzard itself.” The initial attack began back in November and, months later, has left the top tier of Microsoft communications exposed.