



# Daily Threat Bulletin

13 March 2025

## Vulnerabilities

### [Fortinet Patches 18 Vulnerabilities](#)

SecurityWeek - 12 March 2025 13:47

Fortinet has published 17 new advisories to inform customers about 18 vulnerabilities patched in its products.

### [iOS 18.3.2 Patches Actively Exploited WebKit Vulnerability](#)

Infosecurity Magazine - 12 March 2025 18:00

iOS 18.3.2 patches actively exploited WebKit flaw, addressing critical security risks for users

### [Zoom Patches 4 High-Severity Vulnerabilities](#)

SecurityWeek - 12 March 2025 16:00

Zoom has patched five vulnerabilities in its applications, including four high-severity flaws.

### [Facebook discloses FreeType 2 flaw exploited in attacks](#)

BleepingComputer - 12 March 2025 18:04

Facebook is warning that a FreeType vulnerability in all versions up to 2.13 can lead to arbitrary code execution, with reports that the flaw has been exploited in attacks.

## Threat actors and malware

### [China-linked APT UNC3886 targets EoL Juniper routers](#)

Security Affairs - 13 March 2025 00:26

In mid-2024, Mandiant identified custom backdoors on Juniper Networks' Junos OS routers, and attributed the attacks to a China-linked espionage group tracked as UNC3886.

### [Over 400 IPs Exploiting Multiple SSRF Vulnerabilities in Coordinated Cyber Attack](#)

The Hacker News - 12 March 2025 18:26

Threat intelligence firm GreyNoise is warning of a "coordinated surge" in the exploitation of Server-Side Request Forgery (SSRF) vulnerabilities spanning multiple platforms. At least 400 IPs have been seen actively exploiting multiple SSRF CVEs simultaneously, with notable overlap between attack attempts.



Scottish  
Cyber  
Coordination  
Centre

### **New North Korean Android spyware slips onto Google Play**

BleepingComputer - 12 March 2025 14:35

A new Android spyware named 'KoSpy' is linked to North Korean threat actors who have infiltrated Google Play and third-party app store APKPure through at least five malicious apps.

### **#StopRansomware: Medusa Ransomware**

CISA Advisories -

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint advisory to disseminate known Medusa ransomware TTPs and IOCs, identified through FBI investigations as recently as February 2025.