Scottish Cyber Coordination Centre

# Daily Threat Bulletin

19 March 2025

## Vulnerabilities

### New Windows zero-day exploited by 11 state hacking groups since 2017

BleepingComputer - 18 March 2025 14:11

At least 11 state-backed hacking groups from North Korea, Iran, Russia, and China have been exploiting a new Windows vulnerability in data theft and cyber espionage zero-day attacks since 2017. [...]

### U.S. CISA adds Fortinet FortiOS/FortiProxy and GitHub Action flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 March 2025 07:15

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Fortinet FortiOS/FortiProxy and GitHub Action flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog.

### Critical mySCADA myPRO Flaws Could Let Attackers Take Over Industrial Control Systems

The Hacker News - 19 March 2025 13:29

Cybersecurity researchers have disclosed details of two critical flaws impacting mySCADA myPRO, a Supervisory Control and Data Acquisition (SCADA) system used in operational technology (OT) environments, that could allow malicious actors to take control of susceptible systems.

### CISA Warns of Active Exploitation in GitHub Action Supply Chain Compromise

The Hacker News - 19 March 2025 11:35

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a vulnerability linked to the supply chain compromise of the GitHub Action, tj-actions/changed-files, to its Known Exploited Vulnerabilities (KEV) catalog.

### New Critical AMI BMC Vulnerability Enables Remote Server Takeover and Bricking

The Hacker News - 18 March 2025 20:01

A critical security vulnerability has been disclosed in AMI's MegaRAC Baseboard Management Controller (BMC) software that could allow an attacker to bypass authentication and carry out post-exploitation actions.The vulnerability, tracked as CVE-2024-54085, carries a CVSS v4 score of 10.0, indicating maximum severity.

Scottish Cyber Coordination Centre

## Threat actors and malware

### GitHub Action hack likely led to another in cascading supply chain attack

BleepingComputer - 18 March 2025 17:03

A cascading supply chain attack that began with the compromise of the “reviewdog/action-setup@v1” GitHub Action is believed to have led to the recent breach of “tj-actions/changed-files” that leaked CI/CD secrets. [...]

### New ‘Rules File Backdoor’ Attack Lets Hackers Inject Malicious Code via AI Code Editors

The Hacker News - 18 March 2025 22:13

Cybersecurity researchers have disclosed details of a new supply chain attack vector dubbed Rules File Backdoor that affects artificial intelligence (AI)-powered code editors like GitHub Copilot and Cursor, causing them to inject malicious code.

### China-Linked MirrorFace Deploys ANEL and AsyncRAT in New Cyber Espionage Operation

The Hacker News - 18 March 2025 16:54

Threat hunters have shed more light on a previously disclosed malware campaign undertaken by the China-aligned MirrorFace threat actor that targeted a diplomatic organization in the European Union with a backdoor known as ANEL.

### Black Basta Leader in League With Russian Officials, Chat Logs Show

darkreading - 18 March 2025 19:05

Though the chat logs were leaked a month ago, analysts are now seeing that Russian officials may have assisted Black Basta members according, to the shared messages.

### 11 State-Sponsored APTs Exploiting LNK Files for Espionage, Data Theft

SecurityWeek - 18 March 2025 15:00

ZDI has uncovered 1,000 malicious .lnk files used by state-sponsored and cybercrime threat actors to execute malicious commands.

## UK related

### UK wants dirt on data brokers before criminals get there first

The Register - 18 March 2025 11:32

Govt yearns to learn mistakes of serially breached record holders so it can, er, liberalize data sharing regs The UK government is inviting experts to provide insights about the data brokerage industry and the potential risks it poses to national security as it moves to push new data-sharing legislation over the line....