



# Daily Threat Bulletin

31 December 2025

## Vulnerabilities

### [CSA Issues Alert on Critical SmarterMail Bug Allowing Remote Code Execution](#)

**CISA Alert - CVE-2025-52691 - CVSS score of 10.**

The Cyber Security Agency of Singapore (CSA) has issued a bulletin warning of a maximum-severity security flaw in **SmarterTools SmarterMail email software** that could be exploited to achieve remote code execution. The vulnerability, tracked as CVE-2025-52691, **carries a CVSS score of 10.0**. It relates to a case of arbitrary file upload that could enable code execution without requiring any

### [CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories - CVE-2023-52163

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2023-52163 Digiever DS-2105 Pro Missing Authorisation.

### [CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories - CVE-2018-4063

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2018-4063 Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type.

## Threat actors and malware

### [New ErrTraffic service enables ClickFix attacks via fake browser glitches](#)

A new cybercrime tool called ErrTraffic allows threat actors to automate ClickFix attacks by generating 'fake glitches' on compromised websites to lure users into downloading payloads or following malicious instructions

### [US cybersecurity experts plead guilty to BlackCat ransomware attacks](#)

Two former employees of cybersecurity incident response companies Sygnia and DigitalMint have pleaded guilty to targeting U.S. companies in BlackCat (ALPHV) ransomware attacks in 2023.

### [How does AI decision making help companies stay ahead of threats](#)

Security Boulevard - 30 December 2025 23:00



Scottish  
Cyber  
Coordination  
Centre

How Do Non-Human Identities Shape Our Approach to Cybersecurity? Are you aware of how machine identities are silently reshaping cybersecurity? With the rise of Non-Human Identities (NHIs), the traditional approach to cybersecurity needs a significant shift. These NHIs, such as machine identities, are pivotal in forming a robust defense line against potential threats.

### [Chinese APT Mustang Panda Caught Using Kernel-Mode Rootkit](#)

The threat actor uses a signed driver file containing two user-mode shellcodes to execute its ToneShell backdoor. The post Chinese APT Mustang Panda Caught Using Kernel-Mode Rootkit appeared first on SecurityWeek.

## **UK related**

### [Cybersecurity pros admit to moonlighting as ransomware scum](#)

A ransomware negotiator and a security incident response manager have admitted to running ransomware attacks. The October 20225 indictments of Ryan Clifford Goldberg, Kevin Tyler Martin, and an unnamed third co-conspirator, who authorities believe ran a ransomware racket. On Monday, Goldberg and Martin pleaded guilty to one count of conspiracy to obstruct, delay, or affect commerce or the movement of any article or commodity in commerce by extortion. According to a Justice Department the two men and their co-conspirator agreed to pay administrators of the ALPHV BlackCat ransomware 20 percent of any ransom payments they secured, in return for use of the crimeware.