U.S. CISA adds Adminer, Cisco IOS, Fortra GoAnywhere MFT, Libraesva E

Data: 2025-09-30 10:01:50

Autor: Inteligência Against Invaders

U.S. CISA adds Adminer, Cisco IOS, Fortra GoAnywhere MFT, Libraesva ESG, and Sudo flaws to its Known Exploited Vulnerabilities catalog

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Adminer, Cisco IOS, Fortra GoAnywhere MFT, Libraesva ESG, and Sudo flaws to its Known Exploited Vulnerabilities catalog.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA)added Adminer, Cisco IOS, Fortra GoAnywhere MFT, Libraesva ESG, and Sudo flaws to its Known Exploited Vulnerabilities (KEV) catalog.

Below are the descriptions for these flaws:

- CVE-2021-21311Adminer Server-Side Request Forgery Vulnerability
- CVE-2025-20352Cisco IOS and IOS XE Stack-based Buffer Overflow Vulnerability
- CVE-2025-10035Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability
- CVE-2025-59689Libraesva Email Security Gateway Command Injection Vulnerability
- CVE-2025-32463Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability

Last week, Cisco fixed the actively exploited zero-day CVE-2025-20352, impacting Cisco IOS and IOS XE Software. The high-severity vulnerability resides in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and IOS XE Software.

The flaw allows remote authenticated attackers to trigger a DoS condition with low privileges or achieve root code execution with high privileges. An attacker could exploit the flaw by sending a crafted SNMP packet to a vulnerable device over IPv4 or IPv6 networks. The root cause of this vulnerability is a stack overflow condition in the SNMP subsystem of the affected software. The vulnerability impacts all devices with SNMP enabled.

The company Product Security Incident Response Team (PSIRT) is aware of attacks in the wild exploiting this vulnerability.

Another flaw added to the KeV catalog is the vulnerability CVE-2025-10035. Last week, cybersecurity firm watchTowr Labs revealed that it has ‘credible evidence’ that the critical Fortra GoAnywhere MFT flawCVE-2025-10035was actively exploited in attacks in the wild as early as September 10, 2025, a week before it was publicly disclosed.

Fortra GoAnywhere Managed File Transfer is a comprehensive solution for secure file transfer, data

encryption, and compliance management. It provides a centralized platform for managing and automating file transfers between disparate systems and applications, enabling secure and controlled data movement across an organization's network.

On September 18, Fortraaddresseda critical vulnerability, tracked as CVE-2025-10035 (CVSS score of 10.0) in GoAnywhere Managed File Transfer (MFT) software.

The flaw is a deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT. An attacker could exploit the vulnerability to execution of arbitrary commands on the affected systems.

*"A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection."*reads the advisory*.*

The company urges customers to upgrade to a patched version (the latest release 7.8.4, or the Sustain Release 7.6.3).

To mitigate the vulnerability, Fortra recommends restricting public access to the GoAnywhere Admin Console, as exploitation depends on internet exposure.

CISA also added vulnerability CVE-2025-59689 to the catalog after Libraesva reported that nation-state actors exploited the command injection flaw in its Email Security Gateway.

Libraesva Email Security Gateway is an advanced secure email gateway (SEG) solution developed by the Italian cybersecurity company Libraesva.It's designed to protect organizations against email-borne threats, including Spam and phishing emails, Business email compromise (BEC) attempts, Malware and ransomware delivered via attachments or links, Advanced persistent threats (APTs) leveraging email as an entry point.

An attacker could trigger the vulnerability by sending malicious emails containing specially crafted compressed attachments. The flaw lets attackers run arbitrary commands as a non-privileged user due to improper sanitization of code in certain compressed archives.

The company identified at least one incident involving the vulnerability and attributes the attack to a nation-state actor.

In early July, cybersecurity researchers disclosed two vulnerabilities in the Sudo command-line utility for Linux and Unix-like operating systems. Local attackers can exploit the vulnerabilities to escalate privileges to root on affected systems.

Sudo (short for "superuser do") is a command-line utility found in Unix and Linux systems. It lets a permitted user run commands with the security privileges of another user, most commonly the root user (the system's most powerful administrative account).

Below is the description of the two vulnerabilities:

- CVE-2025-32462(CVSS score: 2.8) – Sudo before 1.9.17p1, when used with a sudoers file that specifies a host that is neither the current host nor ALL, allows listed users to execute commands on unintended machines.
- CVE-2025-32463(CVSS score: 9.3) – Sudo before 1.9.17p1 allows local users to obtain root

access because /etc/nsswitch.conf from a user-controlled directory is used with the –chroot option.

The Stratascale Cyber Research Unit (CRU) team discovered both local privilege vulnerabilities.

According toBinding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB agencies have to address the identified vulnerabilities by the due date to protect their networks against attacks exploiting the flaws in the catalog.

Experts also recommend that private organizations review theCatalogand address the vulnerabilities in their infrastructure.

CISA orders federal agencies to fix the vulnerabilities byOctober 20, 2025.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,cisa)