NO.1

AUGUST 1ST 2025

The Cyber Security Chronicle

Weekly Vulnerability Scandal

CISA Warns of Critical Sudo Flaw

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a critical warning about a vulnerability in the sudo utility, **CVE-2025-32463**, which is being actively exploited in the wild to enable local privilege escalation to root on Linux and Unix systems. This flaw, with a CVSS score of 9.3, allows attackers with limited sudo privileges to bypass permission checks and execute arbitrary commands as root. Exploitation relies on the attacker creating a malicious /etc/nsswitch.conf file within a user-specified chroot environment to trick sudo into loading an arbitrary shared library. CISA added CVE-2025-32463 to its Known Exploited Vulnerabilities (KEV) catalog on September 29, 2025, and federal agencies are required to apply mitigations or document a risk acceptance plan by October 20, 2025.

CISA Issues Emergency Directive on Cisco Zero-Days

CISA issued Emergency Directive 25-03 on September 25, 2025, mandating immediate action by federal civilian executive branch agencies to address critical zero-day vulnerabilities in Cisco Adaptive Security Appliances (ASA) and Firepower Threat Defense (FTD) appliances. The vulnerabilities, **CVE-2025-20333** and **CVE-2025-20362**, are being actively exploited by an advanced threat actor linked to the ArcaneDoor campaign, which enables unauthenticated remote code execution and persistence through system reboots and upgrades.

Fortra GoAnywhere MFT Zero-Day Exploited

A critical zero-day vulnerability, CVE-2025-10035, in Fortra's GoAnywhere Managed File Transfer (MFT) software has been actively exploited in the wild. **CVE-2025-10035** - The vulnerability is a deserialization flaw in the License Servlet that enables command injection without authentication, allowing attackers to take full control of affected systems. Evidence indicates exploitation began as early as September 10, 2025, with threat actors using it to create backdoor admin accounts and maintain persistent access. Fortra released the patch on September 18, 2025, but security researchers noted that the company was eight days late in issuing the fix, providing attackers a significant window of opportunity. The flaw is particularly dangerous due to its maximum severity and ease of exploitation, making it a prime target for ransomware operators and advanced persistent threat (APT) groups.

NO.1 AUGUST 1ST 2025

The Cyber Security Chronicle

Weekly Vulnerability Scandal

Google Warns 'Brickstorm' Backdoor

Google has issued a warning about the ongoing use of the sophisticated BRICKSTORM backdoor by China-linked cyber-espionage actors, primarily targeting U.S. legal, technology, Software-as-a-Service (SaaS), and business process outsourcing (BPO) firms since March 2025. The campaign, attributed to the Advanced Persistent Threat (APT) group UNC5221, has enabled attackers to maintain undetected access for an average of 393 days, allowing for prolonged data exfiltration and espionage.

The BRICKSTORM malware, written in Go, is deployed on network appliances like VMware ESXi hypervisors and email gateways that typically lack traditional Endpoint Detection and Response (EDR) coverage, allowing it to evade detection.

Attackers have used a malicious Java Servlet filter called BRICKSTEAL to intercept administrator credentials on VMware vCenter servers and a JSP web shell named SLAYSTYLE to execute arbitrary commands, ensuring persistence and control.

The primary goal of the attacks is the exfiltration of emails via Microsoft Entra ID Enterprise Applications with mail.read or full_access_as_app permissions, which grant access to any mailbox within an organization.

Google's Mandiant division has released a free scanner and YARA rules to help organizations detect BRICKSTORM activity, with experts anticipating that more victims will uncover compromises in the coming one to two years as they conduct network scans.

Fake Microsoft Teams Installers Spread Malware

A sophisticated cyberattack campaign is currently active, where hackers use malvertising and SEO poisoning to distribute fake Microsoft Teams installers that deploy the Oyster backdoor malware. This campaign, reported on September 30, 2025, targets users searching for "Teams download" by redirecting them to spoofed websites like teams-install[.]top, which mimic Microsoft's official download page. The malicious installer, named MSTeamsSetup.exe, appears legitimate and is even signed with valid certificates from entities like "4th State Oy" and "NRM NETWORK RISK MANAGEMENT INC" to bypass security checks. Upon execution, the fake installer drops a malicious DLL file, CaptureService.dll, into the %APPDATA%\Roaming folder and creates a scheduled task named "CaptureService" to run the DLL every 11 minutes, ensuring persistence across reboots. This allows attackers to gain remote access, execute commands, exfiltrate data, and deploy additional payloads, with the malware linked to ransomware groups like Rhysida. The campaign is part of a recurring trend where cybercriminals weaponize trusted software brands to lower infection barriers.

The Oyster malware, also known as Broomstick or CleanUpLoader, has been active since mid-2023 and is used to establish initial access into corporate networks.

NO.1 AUGUST 1ST 2025

The Cyber Security Chronicle

Weekly Vulnerability Scandal

Asahi Group Holdings Cyberattack

Japanese brewing giant Asahi Group Holdings has been hit by a cyberattack that has caused a system failure; halting production, order processing, and shipping operations at its 30 domestic factories in Japan. The company confirmed that no personal information or customer data has been leaked, and its European operations, including those in the UK, remain unaffected.

Harrods Third-Party Data Breach

Luxury department store Harrods has confirmed a significant data breach affecting approximately 430,000 customers, with personal information stolen from a third-party provider's system, not Harrods' own internal networks. The breach, which occurred in late September 2025, involved the compromise of names, contact details, marketing preferences, and loyalty card data, but no payment information or passwords were accessed. Harrods has stated it will not engage with the threat actors who contacted them and has notified relevant authorities, including the Information Commissioner's Office.

UK Government Aid to Jaguar Land Rover

The UK government has secured a £1.5 billion ($2 billion) loan guarantee for Jaguar Land Rover (JLR) to stabilize its supply chain following a cyberattack that halted production across its UK factories since 31 August. This intervention marks the first time the UK government has provided financial assistance to a company specifically due to a cyberattack.

Volvo North America Data Breach

Volvo North America has confirmed the ransomware attack targeted Miljödata, a Swedish IT services provider used by Volvo for HR management, and was claimed by the ransomware group DataCarry. The breach exposed personal data including first and last names, Social Security numbers, email addresses, physical addresses, phone numbers, government IDs, dates of birth, and gender. The attack impacted at least 870,000 accounts across multiple organizations, including Volvo North America, Scandinavian airline SAS, numerous Swedish municipalities, and other companies.

Nation-State Hackers Exploit Libraesva Email Gateway

State-sponsored hackers have actively exploited a critical command injection vulnerability, tracked as **CVE-2025-59689**, in Libraesva's Email Security Gateway (ESG) product, prompting the company to deploy an emergency patch within 17 hours of discovering the abuse. The flaw, which allows attackers to execute arbitrary commands as a non-privileged user by sending a malicious email with a specially crafted compressed attachment, was confirmed to have been used in at least one targeted incident. CVE-2025-59689 is a command injection flaw caused by improper sanitization when processing certain compressed archive formats, allowing attackers to bypass security checks and execute shell commands.