Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

13 December 2023

Vulnerabilities

Sophos backports RCE fix after attacks on unsupported firewalls

Bleeping Computer - December 12 2023

Sophos was forced to backport a security update for CVE-2022-3236 for end-of-life (EOL) firewall firmware versions after discovering hackers actively exploiting the flaw in attacks. The flaw is a code injection problem in the User Portal and Webadmin of Sophos Firewall, allowing remote code execution.

Adobe Releases Security Updates for Multiple Products

CISA Current Activity - December 12 2023

Adobe has released security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following Adobe Security Bulletins and apply the necessary updates.

Apple Releases Security Updates for Multiple Products

CISA Current Activity - December 12 2023

Apple has released security updates for Safari, iOS and iPadOS, Sonoma, Ventura, and Monterey to address multiple vulnerabilities. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following advisories and apply necessary updates: Safari 17.2 iOS 17.2 and iPadOS 17.2 iOS 16.7.3 and iPadOS 16.7.3 macOS Sonoma 14.2 macOS Ventura 13.6.3 macOS Monterey 12.7.2.

Over 1,450 pfSense servers exposed to RCE attacks via bug chain

Bleeping Computer - December 12 2023

Roughly 1,450 pfSense instances exposed online are vulnerable to command injection and cross-site scripting flaws that, if chained, could enable attackers to perform remote code execution on the appliance. pfSense is a popular open-source firewall and router software that allows extensive customization and deployment flexibility.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Over 100 WordPress Repository Plugins Affected by Shortcode-based Stored Cross-Site Scripting

Wordfence - RSS - December 12 2023

On August 14, 2023, the Wordfence Threat Intelligence team began a research project to find Stored Cross-Site Scripting (XSS) via Shortcode vulnerabilities in WordPress repository plugins. This type of vulnerability enables threat actors with contributor-level permissions or higher to inject malicious web scripts into pages using plugin shortcodes, which will execute whenever a victim accesses the injected page. We found over 100 vulnerabilities across 100 plugins which affect over 6 million sites.

Schneider Electric Easy UPS Online Monitoring Software

CISA Current Activity - December 12 2023

Vendor: Schneider Electric Equipment: Easy UPS Online Monitoring Software Vulnerability: Path Traversal 2. RISK EVALUATION Successful exploitation of this vulnerability could allow elevation of privileges which could result in arbitrary file deletion with system privileges.

Microsoft releases lightest Patch Tuesday in three years, no zero-days disclosed

Talos Intelligence Blog - December 12 2023

Microsoft's monthly security update released Tuesday is the company's lightest in four years, including only 33 vulnerabilities. Perhaps more notable is that there are no zero-day vulnerabilities included in December's Patch Tuesday, a rarity for Microsoft this year. The company's regular set of advisories has included a vulnerability that's been actively exploited in the wild in 10 months this year.

UK cyber

UK government risking ‘catastrophic ransomware attack,' parliamentary report warns

Record by Recorded Future - December 13 2023

Because of the British government's failures to tackle ransomware, there is a "high risk" the country faces a "catastrophic ransomware attack at any moment," according to an unprecedentedly critical parliamentary report published Wednesday by the Joint Committee on the National Security Strategy (JCNSS). In particular, the report singles out former Home Secretary Suella Braverman, who it describes as having "showed no interest in the topic" despite her department claiming to be the government lead on the issue as a national security risk and policy matter.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Lazarus Exploits Log4Shell to Deploy Telegram-Based Malware
BankInfoSecurity - December 13 2023

North Korean Hackers Deploy Novel Malware Families North Korean hacking group Lazarus Group is exploiting Log4Shell to target manufacturing, agriculture and physical security sectors, resulting in the deployment of a tailored implant on compromised systems. The attack campaign targeted publicly accessible VMware Horizon servers.