Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

12 December 2023

Vulnerabilities

Apache fixed Critical RCE flaw CVE-2023-50164 in Struts 2

Security Affairs - December 11 2023

The Apache Software Foundation addressed a critical remote code execution vulnerability in the Apache Struts 2 open-source framework. The Apache Software Foundation released security updates to address a critical file upload vulnerability in the Struts 2 open-source framework. Successful exploitation of the flaw, tracked as CVE-2023-50164, could lead to remote code execution.

Atlassian warns of 4 new critical vulnerabilities affecting Jira, Confluence, Bitbucket

SC Magazine US - December 11 2023

Atlassian Jira, Confluence, Bitbucket and macOS Companion app users are warned to update their software immediately due to four critical vulnerabilities allowing for remote code execution (RCE). The Atlassian vulnerabilities disclosed last week are "more likely than not" to be targeted in exploitation campaigns, according to an Australian Cyber Security Centre alert, based on previous exploitation of Jira and Confluence bugs.

50K WordPress sites exposed to RCE attacks by critical bug in backup plugin

Bleeping Computer - December 11 2023

A critical severity vulnerability in a WordPress plugin with more than 90,000 installs can let attackers gain remote code execution to fully compromise vulnerable websites. Known as Backup Migration, the plugin helps admins automate site backups to local storage or a Google Drive account. The security bug (tracked as CVE-2023-6553 and rated with a 9.8/10 severity score) was discovered by a team of bug hunters known as Nex Team, who reported it to WordPress security firm Wordfence under a recently launched bug bounty program.

Apple emergency updates fix recent zero-days on older iPhones

Bleeping Computer - December 11 2023

TLP CLEAR: Disclosure is not limited

Apple has issued emergency security updates to backport patches for two actively exploited zero-day flaws to older iPhones and some Apple Watch and Apple TV models. "Apple is aware of a report that this issue may have been exploited against versions of iOS before iOS 16.7.1," the company said in security advisories published on Monday. The two vulnerabilities, now tracked as CVE-2023-42916 and CVE-2023-42917, were discovered within the WebKit browser engine, developed by Apple and used by the company's Safari web browser across its platforms (e.g., macOS, iOS, iPadOS).

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Current Activity - December 11 2023

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2023-6448 Unitronics Vision PLC and HMI Insecure Default Password.

Malware and threat actors

Two-day water outage in remote Irish region caused by pro-Iran hackers

Record by Recorded Future - December 11 2023

Residents of a remote area on Ireland’s west coast were left without water last week due to a cyberattack perpetrated by a pro-Iran hacking group targeting a piece of equipment the hackers complained was made in Israel. The incident affected a private group water scheme in the rural Erris area of County Mayo, which has a total population of around 8,000 people spread out over just under 1,000 square kilometers — about 0.5% the population of Manhattan in an area 20 times its size. “The attack saw outages for approximately 160 households over two days, and was as a result of the exploitation of a vulnerability in a particular type of programmable logic controller,” a spokesperson for Ireland’s Department of the Environment, Climate and Communications (DECC) told Recorded Future News on Monday.

Report Sees Chinese Threat Actors Embracing Sandman APT

Security Boulevard - RSS - December 11 2023

SentinelLabs, Microsoft and PwC issued an alert that threat actors thought to be associated with cybercriminals based in China adopted an APT known as Sandman to insert malware in IT environments.

Updated GuLoader, DarkGate malware strains emerge

SC Magazine US - December 11 2023

TLP CLEAR: Disclosure is not limited

Continuous improvements have been introduced to the GuLoader and DarkGate malware strains, The Hacker News reports. Despite having little functional modifications since being first discovered in 2019, GuLoader, also known as CloudEyE, has been updated to feature more advanced obfuscation techniques to better evade detection, including updates to its Vectored Exception Handling capability initially uncovered by CrowdStrike, a report from Elastic Security Labs revealed.

Lazarus hackers drop new RAT malware using 2-year-old Log4j bug

Bleeping Computer - December 11 2023

The notorious North Korean hacking group known as Lazarus continues to exploit CVE-2021-44228, aka "Log4Shell," this time to deploy three previously unseen malware families written in DLang. The new malware are two remote access trojans (RATs) named NineRAT and DLRAT and a malware downloader named BottomLoader.