Scottish Cyber Coordination Centre

Daily threat bulletin

2 September 2024

Vulnerabilities

North Korean hackers exploit Chrome zero-day to deploy rootkit

BleepingComputer - 30 August 2024 14:04

North Korean hackers have exploited a recently patched Google Chrome zero-day (CVE-2024-7971) to deploy the FudModule rootkit after gaining SYSTEM privileges using a Windows Kernel exploit. [...]

Fortra fixed two severe issues in FileCatalyst Workflow, including a critical flaw

Security Affairs - 30 August 2024 20:46

Cybersecurity and automation company Fortra addressed two vulnerabilities in FileCatalyst Workflow software, including a critical-severity flaw. Cybersecurity and automation company Fortra released patches for two vulnerabilities in FileCatalyst Workflow. Once of the vulnerabilities is a critical issue, tracked as CVE-2024-6633 (CVSS score of 9.8) described as Insecure Default in FileCatalyst Workflow Setup.

South Korea-linked group APT-C-60 exploited a WPS Office zero-day

Security Affairs - 30 August 2024 12:09

South Korea-linked group APT-C-60 exploited a zero-day in the Windows version of WPS Office to target East Asian countries. South Korea-linked group APT-C-60 exploited a zero-day, tracked as CVE-2024-7262, in the Windows version of WPS Office to deploy the SpyGlace backdoor in the systems on targets in East Asia.

Critical Flaws in Progress Software WhatsUp Gold Expose Systems to Full Compromise

SecurityWeek - 30 August 2024 08:34

Censys warns of over 1,200 internet-accessible WhatsUp Gold instances potentially exposed to malicious attacks.

Published Vulnerabilities Surge by 43%

Infosecurity Magazine - 30 August 2024 14:00

Forescout highlighted a 43% increase in published vulnerabilities in H1 2024, with attackers targeting flaws in VPNs and network infrastructure for initial access

Threat actors and malware

Cicada3301 ransomware's Linux encryptor targets VMware ESXi systems

Scottish Cyber Coordination Centre

BleepingComputer - 01 September 2024 11:14

A new ransomware-as-a-service (RaaS) operation named Cicada3301 has already listed 19 victims on its extortion portal, as it quickly attacked companies worldwide. [...]

New Voldemort malware abuses Google Sheets to store stolen data

BleepingComputer - 30 August 2024 15:04

A campaign that started on August 5, 2024, is spreading a previously undocumented malware named “Voldemort” to organizations worldwide, impersonating tax agencies from the U.S., Europe, and Asia. [...]

GitHub comments abused to push password stealing malware masked as fixes

BleepingComputer - 31 August 2024 12:21

GitHub is being abused to distribute the Lumma Stealer information-stealing malware as fake fixes posted in project comments. [...]

New Malware Masquerades as Palo Alto VPN Targeting Middle East Users

The Hacker News - 30 August 2024 16:50

Cybersecurity researchers have disclosed a new campaign that potentially targets users in the Middle East through malware that disguises itself as Palo Alto Networks GlobalProtect virtual private network (VPN) tool.”