

Weekly Intelligence Summary

Report Date: 10.11.2025

Intelligence Cut-off Date: 07.11.2025

Weekly Focus: Exploitation of CVE-2024-1086 highlights significant gaps in patch management and cyber hygiene

The US government has warned that a long-disclosed Linux vulnerability is now being exploited in ransomware campaigns.

CVE-2024-1086 (OVSS: 90 | CVSS: 7.8) has been exploited by ransomware groups for more than a year, despite being included in the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalogue in May 2024.

CVE-2024-1086 is a use-after-free vulnerability in the Linux kernel's netfilter component, allowing the `nf_tables` module to be exploited for local privilege escalation. The vulnerability was introduced into the Linux kernel via a commit in 2014 and was disclosed in January 2024, with an emergency fix being released the same month. Researchers released a proof-of-concept (PoC) exploit code, also revealing that the flaw affects many major Linux distributions, including Debian, Ubuntu, Fedora, and Red Hat, as well as nearly any distribution with kernel versions from 3.15 to 6.8-rc1.

CISA has recently updated the KEV entry for CVE-2024-1086, disclosing that it has been exploited in ransomware campaigns; however, no further details have been released.

Why It Matters...

The significance of CVE-2024-1086 lies in its ability to grant threat actors root privileges, which can be leveraged to take control of systems, move laterally across networks, and steal sensitive data.

Threat actors continue to target longstanding and well-documented vulnerabilities, highlighting persistent gaps in basic cyber hygiene and patch management. Adversaries also seek to exploit outdated systems, particularly within the manufacturing and healthcare sectors, as well as unpatched software, to achieve a significant impact with minimal effort or innovation, highlighting the reality that many ransomware incidents are easily preventable. Investing in timely vulnerability remediation, asset visibility, and security governance can lead to a substantial reduction in risk.

Kernel components remain an attractive target for threat actors, as they represent a critical weak point that, once exploited, can render security defences ineffective and provide almost undetectable persistence within a system. To mitigate the risk of CVE-2024-1086, it is recommended to update to Linux kernel version 6.8-rc2 or later, which remediates the vulnerability. `nf_tables` can be blocklisted if not actively used, and the Linux Kernel Runtime Guard (LKRG) module can be loaded for protection.

Intelligence Overview

Nation State

Threat actors are distributing a new implant, BADCANDY, to exploit CVE-2023-20198 (OVSS: 96 | CVSS: 10) in the Web UI feature of Cisco IOS XE software. In late 2024, this critical flaw was heavily used by the China-backed actor Salt Typhoon in its campaign against US telecommunication providers.

North Korea has added OtterCookie to its malware toolkit, integrating it with BeaverTail code to produce an evolved module that facilitates credential and cryptocurrency theft. It is also the first nation-state observed using EtherHiding to hide malware on the public blockchain.

Russian operatives continue to use living-off-the-land and dual-use tools to exploit Windows systems in Ukraine. Recent attempts to harvest information used a custom webshell, Localolive, that is associated with Sandworm, a cyberespionage group affiliated with the Russian GRU.

Data Breach

An Australian law firm has disclosed a breach claimed by Anubis ransomware, in which sensitive client information was exfiltrated.

University of Pennsylvania has been impacted by a large-scale email campaign, a multi-system compromise, and data theft affecting 1.2 million individuals.

Japanese media giant Nikkei has confirmed a compromise of its Slack account in which threat actors stole an employee's Slack credentials to expose the names, email addresses, and chat histories of over 17,000 employees and partners.