

# Weekly Intelligence Summary

Report Date: 17.11.2025

Intelligence Cut-off Date: 14.11.2025

**Weekly Focus:** Several critical CVEs have been disclosed in prominent software, presenting both privilege escalation and remote code execution risk.

**Organisations are urged to prioritise patch deployment and monitor impacted technology for anomalous activity, since all three vulnerabilities provide viable pathways for threat actors to elevate privileges or execute arbitrary code.**

Three critical CVEs have been disclosed, impacting the Windows kernel, Watchguard VPN, and Samsung OS. All allow either remote code execution or privilege execution.

[CVE-2025-62215](#) (OVSS: 70 | CVSS: 7.0) impacts [Windows at a kernel level](#), and Microsoft has indicated that this CVE is being actively exploited in the wild, although it requires local access. A patch has been released to address this issue, but systems remain vulnerable until this is applied.

[CVE-2025-9242](#) (OVSS: 76 | CVSS: 9.8) is an [out-of-bounds vulnerability in WatchGuard Fireware OS](#). This allows remote code execution during the handshake process to establish a VPN tunnel.

[CVE-2025-21042](#) (OVSS:77 | CVSS:9.8) is a flaw in [Samsung's image-processing library](#), which threat actors are leveraging via embedded zip archives in malformed .DNG raw files, potentially allowing remote code execution and full device access.

## Why It Matters...

Although these are technical vulnerabilities, successful exploitation still often depends on user interaction or weak security practices. For example, in the Windows case, a threat actor must already have local access, which is likely gained through breached credentials or user-level phishing. Similarly, exploitation of the Samsung flaw relies on users interacting with images from untrusted or unknown sources as a key step in the attack chain.

Bring-your-own-device (BYOD) also presents additional risk, particularly for Samsung devices, as organisations often lack full oversight of personal endpoints. This can allow vulnerable devices to remain connected to the wider corporate network and bypass standard security governance.

Organisations should provide targeted security awareness training so users understand the risks and recognise attempts to coerce them into interacting with seemingly legitimate services or content. They should also maintain visibility over their full attack surface, particularly where shadow IT and BYOD are present, and ensure these endpoints are incorporated into standard patching and vulnerability management processes.

## Intelligence Overview

### Malicious Insider

[A former Intel software engineer downloaded 18,000 confidential company files](#) just days before he was due to be dismissed. Although a first attempted unauthorised file transfer was blocked by Intel's security measures, a second attempt was successful despite triggering internal investigation protocols.

### Cybercrime

Threat actors have been targeting the hospitality industry worldwide, using compromised Booking.com accounts to deliver spear-phishing emails and [ClickFix techniques to deploy PureRAT malware](#) for data exfiltration.

The [Rhadamanthys Malware-as-a-Service](#) (MaaS) operation has experienced significant disruption after subscribers lost access to its web interface. The interruption is believed to be tied to an upcoming law enforcement campaign dubbed Operation Endgame.

Suspected criminal threat actors are [disguising legitimate RMM platform downloads](#) as utilities such as 7-Zip & Notepad++ to compromise endpoints and deliver the PatoRAT backdoor.

### CL0P Ransomware

The [Washington Post](#) is the latest high-profile organisation to confirm being impacted by Cl0p's Oracle E-business Suite (EBS) campaign. The media outlet has not disclosed how many files were stolen or what systems may have been compromised.