AL2025_26 WinRAR Vulnerability CVE-2025-31334: MotW Security Bypass (April 7th, 2025)

Description

A newly disclosed vulnerability in WinRAR, tracked as CVE-2025-31334, allows attackers to bypass Windows' Mark of the Web (MotW) security mechanism. This flaw affects all WinRAR versions prior to 7.11 and could allow malicious actors to execute arbitrary code on targeted systems without triggering typical Windows security alerts. The issue revolves around how WinRAR handles symbolic links (symlinks) when extracting and launching executable files. MotW is a security feature that tags files downloaded from the internet with metadata (zone-identifier) indicating potential risk. Windows then uses this data to prompt users before executing the file. This vulnerability effectively disables that protection in specific scenarios.

Attack Details

CVE-2025-31334 involves the use of specially crafted symbolic links inside WinRAR archives. When such a symlink points to an executable and is launched via the WinRAR shell, the MotW metadata is ignored, resulting in no security warning prompt from Windows. This allows attackers to stealthily execute malicious payloads without user suspicion. Notably, symlinks can only be created on Windows systems with administrator privileges, which slightly reduces the risk surface. However, it is a viable vector in scenarios where the attacker has admin access or can trick users into running crafted archives. This vulnerability is particularly concerning given its similarity to previously exploited flaws, such as the 7-Zip double-archiving MotW bypass used to deploy Smokeloader malware. Nation-state threat actors have been known to leverage such weaknesses for stealthy malware delivery.

Remediation

To mitigate and prevent exploitation of this vulnerability, follow these steps:

- Update WinRAR to version 7.11 or later. The latest release includes a fix for CVE-2025-31334.
- Block or restrict execution of symbolic links, particularly in environments where users have elevated privileges.

- Disable or monitor the use of WinRAR shell execution, especially for unknown or internet-downloaded archives.
- Educate users about the risks of opening suspicious archives, particularly those from untrusted sources.
- Use endpoint protection tools to flag unusual archive behavior, especially if executables run without security prompts.
- Consider implementing application whitelisting to restrict unauthorized executables from launching.
- Monitor system logs and network traffic for anomalies related to RAR extraction and execution.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Ilascu, I. (2025, April 4). WinRAR flaw bypasses Windows Mark of the Web security alerts. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/winrar-flaw-bypasses-windows-mark-of-the-web-security-alerts/
- NVD - CVE-2025-31334. (n.d.). Retrieved from National Vulnerability Database https://nvd.nist.gov/vuln/detail/CVE-2025-31334