AL2025_14 WinRAR 7.10 Enhances Privacy by Stripping Metadata from Mark-of-the-Web (27th February 2025)

Description

WinRAR 7.10, the latest version of the popular file compression and archiving tool, introduces several new features, including dark mode, larger memory pages for improved performance, and a revamped settings interface. A particularly notable update is the ability to fine-tune the propagation of Windows' Mark-of-the-Web (MoTW) flags when extracting files. This update enhances user privacy by stripping metadata such as download locations and IP addresses, while still maintaining security features.

Attack Details

Mark-of-the-Web (MoTW) is an alternate data stream named "Zone.Identifier" added to files downloaded from the Internet. It serves as an important security mechanism in Windows, warning users about potentially risky files and allowing Microsoft Office to open documents in Protected View. Cybercriminals often exploit vulnerabilities in MoTW implementations to bypass security measures and execute malicious files without warning.

Threat actors typically attempt to evade MoTW protections using zero-day flaws or by modifying extracted files to remove security warnings. The new WinRAR setting allows users to strip sensitive metadata from the MoTW stream, making it more difficult for forensic analysts to trace a file's origin. While this change enhances privacy, it may also hinder investigative efforts in tracking malicious files.

Remediation

- **Configure MoTW Propagation Wisely**: Users should assess their security needs and configure WinRAR settings accordingly. If full MoTW data is required, go to WinRAR Settings > Security and uncheck "Zone value only."
- **Verify Download Sources:** Always ensure files come from trusted sources before extracting them, as MoTW stripping may hide a file's origin.
- **Use Advanced Endpoint Protection:** Deploy security solutions that can detect malicious activity even in cases where MoTW metadata is missing.
- **Regularly Update Software:** Keep WinRAR and other security tools updated to benefit from the latest security improvements and mitigations.
- **Enable File Execution Warnings:** Configure Windows to prompt warnings for unknown or newly downloaded executables, even if MoTW metadata is stripped.

While WinRAR 7.10’s privacy-focused update is beneficial for users concerned about data exposure, security teams should remain vigilant about the potential implications of metadata stripping. Balancing privacy and security will be crucial in effectively managing extracted files.

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

References

- Abrams, L. (2025, February 19). New WinRAR version strips Windows metadata to increase privacy. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-winrar-version-strips-windows-metadata-to-increase-privacy/
- GmbH, W. (n.d.). WinRAR 7.11 Beta 1 released. Retrieved from WinRAR Latest News. https://www.win-rar.com/singlenewsview.html?&L=0