Security Advisory 2022-063

Path Traversal Vulnerability in Unrar affects Zimbra software

August 31, 2022 — v1.0

TLP:WHITE

History:

• 31/08/2022 — v1.0 – Initial publication

Summary

In May 2022, security research team from SonarSource discovered a 0-day vulnerability in the unrar utility for Linux and Unix systems. This utility is a third party tool used in Zimbra. The exploitation of this vulnerability allows a remote attacker to execute arbitrary code on a vulnerable Zimbra instance without requiring any prior authentication or knowledge about it. [1]

Proof of Concepts (POC) are now publicly available as well as a metasploit module.

Details

The vulnerability is identified as CVE-2022-30333 and has a severity score of 7.5 out of 10. [2]

The main issue here is with how unrar handles symbolic links. Specifically, it validates that Linux symbolic links don’t contain path traversal characters using forward-slash characters (../), then converts Windows symbolic links (with backslash characters) to Linux. That is, it performs security checks before converting data. As a result, a malicious Windows symbolic link can bypass Linux’s protections and point to anywhere on the Linux filesystem [4]

Regarding Zimbra software, it uses a tool called Amavis, an open-source content filter to provide protection against spam and viruses and other malware. Amavis uses unrar utility to inspect .rar files.

Once the vulnerability is exploited on Zimbra instance, the attacker can execute arbitrary system commands as the zimbra user.
Affected Products

The official security patch by RarLab is contained in the UnRar source code version 6.1.7 and is included with the binaries of version 6.12. Any previous version may be vulnerable, which is used by:

- Zimbra 9.0.0 patch 24 and earlier
- Zimbra 8.8.15 patch 31 and earlier
- Possibly older versions

Recommendations

As of the most recent Zimbra patches, Amavis uses 7z instead. CERT-EU strongly recommends applying the latest updates of Zimbra as soon as possible on. [5]

References

[1] https://blog.sonarsource.com/zimbra-pre-auth-rce-via-unrar-0day/