Security Advisory 2022-069

Remote Code Execution in Zimbra Collaboration Suite

October 7, 2022 — v1.1

TLP:CLEAR

History:

- 07/10/2022 — v1.0 – Initial publication
- 14/10/2022 — v1.1 – Updated with patch

Summary

In September 2022, a remote code execution vulnerability similar to CVE-2022-30333 (SA2022-063) was reported for Zimbra Collaboration Suite. Tracked as CVE-2022-41352 since September 25, 2022, this yet-unpatched flaw is due to an unsafe use of a vulnerable cpio utility by the Zimbra’s antivirus engine Amavis. The exploitation of this vulnerability allows a remote unauthenticated attacker to execute arbitrary code on a vulnerable Zimbra instance.

Proof of Concepts (POC) are publicly available for this vulnerability and reported actively exploited [1].

Technical Details

This 9.8 out of 10 vulnerability allows an unauthenticated attacker to upload arbitrary files by emailing a .cpio, .tar or .rpm to an affected server [2].

Upon reception, the Amavis antivirus engine uses the cpio utility to extract the untrusted received file. Due to the use of vulnerable version of cpio (CVE-2015-1197) on affected systems [3], the attacker can leverage this deflating step and virtually write to any path on the system where the zimbra user has access. This allows the attacker to create and overwrite files on the Zimbra server, including the webroot, which can effectively give him remote code execution [4].

This exploit can be chained with another existing vulnerability (CVE-2022-37393) to escalate to root privileges and achieve a complete remote overtake of a Zimbra server [5].
Affected Products

By default the Amavis engine uses the pax utility and only calls cpio as a fallback if pax does not exist. The systems where pax is installed are thus not affected. The presence of a vulnerable version of cpio is also needed for the exploitation, which might be the case on most systems [6].

On Ubuntu systems, pax should already be installed as a dependency of Zimbra. Red-Hat based deployments are likely to be vulnerable since the utility is not installed by default.

The following Linux distributions were tested by Rapid7 [6]:

• Oracle Linux 8 – vulnerable
• Red Hat Enterprise Linux 8 – vulnerable
• Rocky Linux 8 – vulnerable
• CentOS 8 – vulnerable
• Ubuntu 20.04 – not vulnerable
• Ubuntu 18.04 – not vulnerable

Recommendations

Updates of 14/10/2022

A patch to fix this vulnerability as well as CVE-2022-37393 and CVE-2022-41348 is now available [7]. CERT-EU strongly recommends applying it.

References