CERT-EU

Security Advisory 2023-011

ClamAV critical vulnerability

February 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/02/2023 — v1.0 – Initial publication*

Summary

On February 15th, 2023, ClamAV informed about a critical vulnerability in the cross-platform antimalware toolkit [1]. The vulnerability is identified as `CVE-2023-20032` and could lead to remote code execution.

Technical Details

The vulnerability `CVE-2023-20032` lies in the HFS+ partition file parser of affected ClamAV versions and could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition [2].

Affected Products

The vulnerability affects the following ClamAV versions:

- 0.103.7 and earlier
- 0.105.1 and earlier
- 1.0.0 and earlier

Moreover, ClamAV **0.104 has reached end-of-life** and will not be patched. Anyone using ClamAV 0.104 must switch to a supported version [1].

Recommendations

CERT-EU recommends installing updates on all devices running ClamAV as soon as possible [1].

References

[1] https://blog.clamav.net/2023/02/clamav-01038-01052-and-101-patch.html?m=1

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy