CVE-ID

CVE-2017-1000249 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue in file() was introduced in commit 9611f31313a93aa036389c5f3b15eea53510d4d1 (Oct 2016) lets an attacker overwrite a fixed 20 bytes stack buffer with a specially crafted .notes section in an ELF binary. This was fixed in commit 35c94dc6acc418f1ad7f6241a6680e5327495793 (Aug 2017).

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://github.com/file/file/commit/35c94dc6acc418f1ad7f6241a6680e5327495793
- CONFIRM:https://github.com/file/file/commit/9611f31313a93aa036389c5f3b15eea53510d4d
- DEBIAN:DSA-3965
- URL:http://www.debian.org/security/2017/dsa-3965
- GENTOO:GLSA-201710-02
- URL:https://security.gentoo.org/glsa/201710-02

Assigning CNA

MITRE Corporation

Date Entry Created

20170911 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20170911)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)