



CVE-2025-27363

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-27363 |
| State | PUBLISHED |
| Assigner | facebook |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-03-11 14:15:25 UTC |
| Updated | 2026-04-16 19:16:31 UTC |
| Description | An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) wher |

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.634390000 probability, percentile 0.984160000 (date 2026-04-16)

CISA KEV: Listed on 2025-05-06; due 2025-05-27; ransomware use Unknown

Problem Types: CWE-787 | Out-of-bounds Write (CWE-787) | CWE-787 CWE-787 Out-of-bounds Write

| Version | Source | Type | Score | Severity | Vector |
|---------|-------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 8.1 | HIGH | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | cve-assign@fb.com | Secondary | 8.1 | HIGH | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 8.1 | HIGH | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

| | |
|------------------------|--|
| Vendor | FreeType |
| Product | FreeType |
| Name | FreeType Out-of-Bounds Write Vulnerability |
| Required Action | Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. |
| Notes | This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://source.android.com/docs/security/bulletin/2025-05-01 ; https://nvd.nist.gov/vuln/detail/CVE-2025-27363 |

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|----------|--------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 11.0 | All | All | All |
| Application | Freetype | Freetype | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|----------|----------|------------------------------|---------------|
| CNA | FreeType | FreeType | affected 0.0.0 2.13.0 semver | Not specified |

References

| Reference | Source | Link | Tags |
|---|--------------------------------------|---|-------------|
| www.openwall.com/lists/oss-security/2025/03/13/8 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2026/04/16/5 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | |
| www.openwall.com/lists/oss-security/2025/03/13/12 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| source.android.com/docs/security/bulletin/2025-05-01 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | source.android.com | Third Part |
| www.openwall.com/lists/oss-security/2025/03/13/11 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.facebook.com/security/advisories/cve-2025-27363 | cve-assign@fb.com | www.facebook.com | Third Part |
| lists.debian.org/debian-lts-announce/2025/03/msg00030.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/03/13/1 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |

| | | | |
|--|--------------------------------------|------------------|-------------|
| www.openwall.com/lists/oss-security/2025/03/13/2 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.cisa.gov/known-exploited-vulnerabilities-catalog | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | www.cisa.gov | US Gover |
| www.openwall.com/lists/oss-security/2025/03/13/3 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/03/14/4 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/03/14/3 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/03/14/2 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/03/14/1 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| www.openwall.com/lists/oss-security/2025/05/06/3 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com | Mailing Lis |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, |
| CISA Known Exploited Vulnerabilities catalog | CISA | www.cisa.gov | kev |

No vendor comments have been submitted for this CVE.

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------------------|
| ADP | 2025-05-06T00:00:00.000Z | CVE-2025-27363 added to CISA KEV |

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)