CVE-2026-35233

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-35233
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 18:16:14 UTC
Updated	2026-05-05 17:46:30 UTC
Description	An unprivileged attacker can craft a user-space process with a malicious ELF binary containing an out-of-range sh_link fielc

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from secalert_us@oracle.com

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

EPSS: 0.000130000 probability, percentile 0.021650000 (date 2026-05-05)

Problem Types: CWE-125 | An unprivileged attacker can craft a user-space process with a malicious ELF binary containing an out-of-range sh_link field. When root-level dtrace attaches to -- or instruments -- that process (via dtrace -p , pid probes, or USDT), the ELF parser reads heap memory beyond the allocated section cache array without any bounds check. This results in an uninitialized/out-of-bounds heap read that can cause a NULL pointer dereference crash of the dtrace process (DoS), or -- depending on heap layout -- a read-then-use of a garbage pointer controlled by adjacent allocations, providing a foothold toward further exploitation in a privileged context. | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Linux	10	0	All	All
Operating System	Oracle	Linux	8	-	All	All
Operating System	Oracle	Linux	9	0	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Oracle Linux	affected 8	Not specified
CNA	Oracle Corporation	Oracle Linux	affected 9	Not specified
CNA	Oracle Corporation	Oracle Linux	affected 10	Not specified

References

Reference	Source	Link	Tags
linux.oracle.com/cve/CVE-2026-35233.html	secalert_us@oracle.com	linux.oracle.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**