GNU Binutils objdump debug.c debug_type_samep memory corruption

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

Summary

CVE	CVE-2025-5245
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-27 15:15:36 UTC
Updated	2026-05-12 13:17:23 UTC
Description	A vulnerability classified as critical has been found in GNU Binutils up to 2.44. This affects the function debug_type_samep

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000840000 probability, percentile 0.242330000 (date 2026-05-12)

Problem Types: CWE-119 | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
2.0	cna@vuldb.com	Secondary	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Binutils	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GNU	Binutils	affected 2.0	Not specified
CNA	GNU	Binutils	affected 2.1	Not specified
CNA	GNU	Binutils	affected 2.2	Not specified
CNA	GNU	Binutils	affected 2.3	Not specified
CNA	GNU	Binutils	affected 2.4	Not specified
CNA	GNU	Binutils	affected 2.5	Not specified
CNA	GNU	Binutils	affected 2.6	Not specified
CNA	GNU	Binutils	affected 2.7	Not specified
CNA	GNU	Binutils	affected 2.8	Not specified
CNA	GNU	Binutils	affected 2.9	Not specified
CNA	GNU	Binutils	affected 2.10	Not specified
CNA	GNU	Binutils	affected 2.11	Not specified
CNA	GNU	Binutils	affected 2.12	Not specified
CNA	GNU	Binutils	affected 2.13	Not specified
CNA	GNU	Binutils	affected 2.14	Not specified

CNA	GNU	Binutils	affected 2.15	Not specified
CNA	GNU	Binutils	affected 2.16	Not specified
CNA	GNU	Binutils	affected 2.17	Not specified
CNA	GNU	Binutils	affected 2.18	Not specified
CNA	GNU	Binutils	affected 2.19	Not specified
CNA	GNU	Binutils	affected 2.20	Not specified
CNA	GNU	Binutils	affected 2.21	Not specified
CNA	GNU	Binutils	affected 2.22	Not specified
CNA	GNU	Binutils	affected 2.23	Not specified
CNA	GNU	Binutils	affected 2.24	Not specified
CNA	GNU	Binutils	affected 2.25	Not specified
CNA	GNU	Binutils	affected 2.26	Not specified
CNA	GNU	Binutils	affected 2.27	Not specified
CNA	GNU	Binutils	affected 2.28	Not specified
CNA	GNU	Binutils	affected 2.29	Not specified
CNA	GNU	Binutils	affected 2.30	Not specified
CNA	GNU	Binutils	affected 2.31	Not specified
CNA	GNU	Binutils	affected 2.32	Not specified
CNA	GNU	Binutils	affected 2.33	Not specified
CNA	GNU	Binutils	affected 2.34	Not specified
CNA	GNU	Binutils	affected 2.35	Not specified
CNA	GNU	Binutils	affected 2.36	Not specified
CNA	GNU	Binutils	affected 2.37	Not specified
CNA	GNU	Binutils	affected 2.38	Not specified
CNA	GNU	Binutils	affected 2.39	Not specified
CNA	GNU	Binutils	affected 2.40	Not specified
CNA	GNU	Binutils	affected 2.41	Not specified
CNA	GNU	Binutils	affected 2.42	Not specified
CNA	GNU	Binutils	affected 2.43	Not specified
CNA	GNU	Binutils	affected 2.44	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom	Not specified

ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

References

Reference	Source	Link	Tags
sourceware.org/bugzilla/show_bug.cgi	cna@vuldb.com	sourceware.org	Exploit, Iss
sourceware.org/git/gitweb.cgi	cna@vuldb.com	sourceware.org	Product
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
sourceware.org/bugzilla/attachment.cgi	cna@vuldb.com	sourceware.org	Broken Lir
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
vuldb.com	cna@vuldb.com	vuldb.com	Third Party
vuldb.com	cna@vuldb.com	vuldb.com	Permissior
www.gnu.org	cna@vuldb.com	www.gnu.org	Product
vuldb.com	cna@vuldb.com	vuldb.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: lcyf-fizz (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-05-27T00:00:00.000Z	Advisory disclosed
CNA	2025-05-27T02:00:00.000Z	VulDB entry created
CNA	2025-05-27T10:12:17.000Z	VulDB entry last update

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