



nscd: netgroup cache assumes NSS callback uses in-buffer strings

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

Summary

CVE	CVE-2024-33602
State	PUBLISHED
Assigner	glibc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-06 20:15:11 UTC
Updated	2026-05-12 12:16:35 UTC
Description	nscd: netgroup cache assumes NSS callback uses in-buffer strings The Name Service Cache Daemon's (nscd) netgroup ca

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from ADP

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

Problem Types: CWE-466 | CWE-466 CWE-466 Return of Pointer Value Outside of Expected Range

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Netapp	Element Software	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Operating System	Netapp	Hci Bootstrap Os	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Solidfire Hci Storage Node	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	The GNU C Library	Glibc	affected 2.15 2.40 custom	Not specified
ADP	Gnu	Glibc	affected 2.15 2.40 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 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	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

References

Reference	Source	Link	Tags
-----------	--------	------	------

lists.debian.org/debian-lts-announce/2024/06/msg00026.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mailin
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
sourceware.org/git	af854a3a-2127-422b-91ae-364da2661108	sourceware.org	Broke
www.openwall.com/lists/oss-security/2024/07/22/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailin
security.netapp.com/advisory/ntap-20240524-0012	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com	Third
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

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