389-ds-base: 389-ds-base: remote code execution and denial of service via heap buffer overflow

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-14905
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-23 16:29:35 UTC
Updated	2026-03-31 16:16:27 UTC
Description	A flaw was found in the 389-ds-base server. A heap buffer overflow vulnerability exists in the `schema_attr_enum_callback`

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from secalert@redhat.com

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

EPSS: 0.004660000 probability, percentile 0.643730000 (date 2026-04-02)

Problem Types: CWE-122 | CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Directory Server 11.5 E4S For RHEL 8	unaffected 8060020260303152239.0ca98e
CNA	Red Hat	Red Hat Directory Server 11.7 E4S For RHEL 8	unaffected 8080020260227193008.f969626
CNA	Red Hat	Red Hat Directory Server 11.9 For RHEL 8	unaffected 8100020260312105752.37ed7c
CNA	Red Hat	Red Hat Directory Server 12.2 E4S For RHEL 9	unaffected 9020020260304180546.1674d5
CNA	Red Hat	Red Hat Directory Server 12.4 EUS For RHEL 9	unaffected 9040020260225135630.1674d5
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.1.3-7.el10_1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 0:3.0.6-17.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:1.3.11.1-11.el7_9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 8100020260312103235.25e700
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 8020020260303204738.dbc46b
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 8040020260303172348.96015a
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 8040020260303172348.96015a
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 8060020260303144613.824efc5
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 8060020260303144613.824efc5
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 8060020260303144613.824efc5
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 8080020260227183930.6dbb38
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 8080020260227183930.6dbb38
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.7.0-10.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.0.14-5.el9_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:2.2.4-17.el9_2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.4.5-24.el9_4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 0:2.6.1-20.el9_6 * rpm
CNA	Red Hat	Red Hat Directory Server 13.1	unaffected sha256:5e49efa2b8764403fad1
CNA	Red Hat	Red Hat Directory Server 12	Not specified
CNA	Red Hat	Red Hat Directory Server 13	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:5512	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6220	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:4720	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5597	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5569	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2025-14905	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5511	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3504	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5196	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5514	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4207	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4661	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5568	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5513	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3189	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3379	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5576	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6268	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3208	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5598	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: This issue was discovered by Red Hat Security Research Team (Red Hat Inc.). (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-18T18:04:56.621Z	Reported to Red Hat.
CNA	2026-02-23T00:00:00.000Z	Made public.

Workarounds

CNA: Restrict network access to the 389-ds-base server to only trusted hosts and networks

using firewall rules. Additionally, ensure that administrative access to the server is strictly limited to authorized personnel with strong authentication, as exploitation requires high privileges. This reduces the attack surface and the likelihood of an attacker gaining the necessary privileges to trigger the heap overflow.

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