Python-kdcproxy: remote dos via unbounded tcp upstream buffering

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

Summary

CVE	CVE-2025-59089
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-12 17:15:38 UTC
Updated	2026-04-20 09:16:08 UTC
Description	If an attacker causes kdcproxy to connect to an attacker-controlled KDC server (e.g. through server-side request forgery), tl

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-770 | CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Latchset	Kdcproxy	affected 1.1.0 semver
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:1.0.0-19.el10_1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 0:1.0.0-19.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:0.3.2-3.el7_9.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 8100020251103113748.143e9e
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 8100020251028161822.823393
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 8020020251106022345.792f406
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 8040020251103205102.5b01ab
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 8040020251103205102.5b01ab
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 8060020251030180424.ada582
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 8060020251030180424.ada582
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 8060020251030180424.ada582
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 8080020251029082621.b0a6ce
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 8080020251029082621.b0a6ce
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:1.0.0-9.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:1.0.0-7.el9_0.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:1.0.0-7.el9_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:1.0.0-7.el9_4.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 0:1.0.0-9.el9_6 * rpm

References

Reference	Source	Link
access.redhat.com/security/cve/CVE-2025-59089	secalert@redhat.com	access.red
access.redhat.com/errata/RHSA-2025:21142	secalert@redhat.com	access.red
github.com/latchset/kdcproxy/pull/68	secalert@redhat.com	github.com
access.redhat.com/errata/RHSA-2025:21820	secalert@redhat.com	access.red
access.redhat.com/errata/RHSA-2025:21819	secalert@redhat.com	access.red
access.redhat.com/errata/RHSA-2025:21141	secalert@redhat.com	access.red
access.redhat.com/errata/RHSA-2025:21821	secalert@redhat.com	access.red

access.redhat.com/errata/RHSA-2025:21818	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:21140	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:21748	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:22982	secalert@redhat.com	access.re
github.com/latchset/kdcproxy/commit/c7675365aa20be11f03247966336c7613cac...	af854a3a-2127-422b-91ae-364da2661108	github.com
access.redhat.com/errata/RHSA-2025:21448	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:21139	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:21138	secalert@redhat.com	access.re
access.redhat.com/errata/RHSA-2025:21806	secalert@redhat.com	access.re
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.re
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Arad Inbar for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-09-08T21:37:15.428Z	Reported to Red Hat.
CNA	2025-11-12T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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