Icu: stack buffer overflow in the srbroot::addtag function

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

Summary

CVE	CVE-2025-5222
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-27 21:15:23 UTC
Updated	2026-04-23 00:16:44 UTC
Description	A stack buffer overflow was found in Internationl components for unicode (ICU). While running the genrb binary, the 'subtag

Risk And Classification

Primary CVSS: v3.1 7 HIGH from secalert@redhat.com

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

Problem Types: CWE-120 | CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
High

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Unicode	International Components For Unicode	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:74.2-5.el10_0 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:67.1-10.el9_6 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:67.1-10.el9_6 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:67.1-10.el9_0 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:67.1-10.el9_2 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:67.1-10.el9_4 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

Reference	Source	Link
unicode-org.atlassian.net/jira/software/c/projects/ICU/issues/ICU-22957	secalert@redhat.com	unicode-org.atlassian.
lists.debian.org/debian-lts-announce/2025/06/msg00015.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
access.redhat.com/errata/RHSA-2025:12331	secalert@redhat.com	access.redhat.com
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com
access.redhat.com/errata/RHSA-2025:11888	secalert@redhat.com	access.redhat.com
access.redhat.com/security/cve/CVE-2025-5222	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:12333	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:12083	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2025:12332	secalert@redhat.com	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-05-26T13:39:54.361Z	Reported to Red Hat.
CNA	2024-11-14T00:00:00.000Z	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.