



# Icu: stack buffer overflow in the srbrroot::addtag function

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

## Summary

<b>CVE</b>	CVE-2025-5222
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-05-27 21:15:23 UTC
<b>Updated</b>	2026-04-23 00:16:44 UTC
<b>Description</b>	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	<b>CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H</b>
3.1	CNA	CVSS	7	HIGH	<b>CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H</b>

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

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

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.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)