

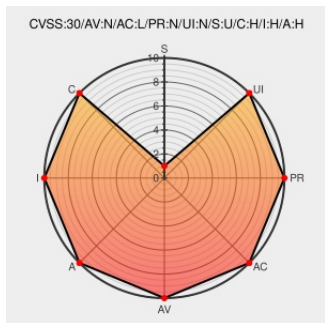


CVE-2014-9911

Published on: 01/04/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9911

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [International Components For Unicode](#) from [Icu-project](#) contain the following vulnerability:

Stack-based buffer overflow in the `ures_getByKeyWithFallback` function in `common/uresbund.cpp` in International Components for Unicode (ICU) before 54.1 for C/C++ allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted `uloc_getDisplayName` call.

CVE-2014-9911 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ICU Stack Overflow in <code>ures_getByKeyWithFallback()</code> Lets Users Execute Arbitrary Code on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTrack 1037556

	text/html	
oss-security - Re: CVE request: icu: stack-based buffer overflow in uloc_getDisplayName	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20161124 Re: CVE request: icu: stack-based buffer overflow in uloc_getDisplayName
Bug 1383569 – CVE-2014-9911 icu: stack-based buffer overflow in uloc_getDisplayName	Issue Tracking Patch Third Party Advisory VDB Entry bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1383569
[ICU-1089] Transliterator methods should take UErrorCode as one of the parameters - Unicode Consortium	Not Applicable bugs.icu-project.org text/html	CONFIRM bugs.icu-project.org/trac/ticket/1089
Changeset 35699 – Unicode ICU trac	Patch Vendor Advisory bugs.icu-project.org text/html	CONFIRM bugs.icu-project.org/trac/changeset/35699
PHP :: Sec Bug #67397 :: Buffer overflow in locale_get_display_name->uloc_getDisplayName (libicu 4.8.1)	Patch Third Party Advisory bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=67397
Oracle Critical Patch Update Advisory - April 2019	www.oracle.com text/html	MISC www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
ICU 'uloc_getDisplayName()' Function Stack Based Buffer Overflow Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94520
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icu-project	International Components For Unicode	All	All	All	All
Application	Icu-project	International Components For Unicode	All	All	All	All
Application	Icu-project	International Components For Unicode	All	All	All	All
cpe:2.3:a:icu-project:international_components_for_unicode:*:*:*:*:c/++:*:*:						
cpe:2.3:a:icu-project:international_components_for_unicode:*:*:*:*:c/c\+\+:*:*:						
cpe:2.3:a:icu-project:international_components_for_unicode:*:*:*:*:c/c\+\+:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#).

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