

Alpine Linux - Bug #6548

Bug # 6547 (Closed): icu: Stack based buffer overflow in locid.cpp (CVE-2016-7415)

[3.5] icu: Stack based buffer overflow in locid.cpp (CVE-2016-7415)

12/19/2016 11:26 AM - Alichu CH

Status: Closed	Start date: 12/19/2016
Priority: Normal	Due date:
Assignee: Natanael Copa	% Done: 100%
Category: Security	Estimated time: 0.00 hour
Target version: 3.5.1	Security IDs:
Affected versions:	
Description	
Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long locale string.	
Fixed In Version:	
icu 58.1	
References:	
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7415 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-7415	
Upstream bug (private):	
http://bugs.icu-project.org/trac/ticket/12745	
No patch available.	

Associated revisions

Revision 383064a7 - 12/26/2016 08:30 AM - Leonardo Arena

main/icu: security upgrade to 58.1 (CVE-2016-7415). Fixes #6548

Revision a32ce150 - 12/27/2016 09:01 AM - Leonardo Arena

main/icu: security fix (CVE-2016-7415). Fixes #6548

(cherry picked from commit 1fa78865839b8c66006d1ae3a0a626e7acc7787d)

History

#1 - 12/22/2016 10:25 AM - Natanael Copa

- Target version changed from 3.5.0 to 3.5.1

#2 - 12/26/2016 08:30 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset [alpine:383064a721ebafed7c65d9e32dc4c6606e95bbd3](https://alpine-linux.org/commits/alpine:383064a721ebafed7c65d9e32dc4c6606e95bbd3).

#3 - 12/29/2016 09:00 AM - Alichu CH

- Category set to Security

- Status changed from Resolved to Closed