

Asterisk Project Security Advisory - AST-2018-003

Product	Asterisk
Summary	Crash with an invalid SDP fmtmp attribute
Nature of Advisory	Remote crash
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	January 15, 2018
Reported By	Sandro Gauci
Posted On	February 21, 2018
Last Updated On	March 8, 2018
Advisory Contact	Kevin Harwell <kharwell AT diguim DOT com>
CVE Name	CVE-2018-1000099

Description	<p>By crafting an SDP message body with an invalid fmtmp attribute Asterisk crashes when using the pjsip channel driver because pjproject's fmtmp retrieval function fails to check if fmtmp value is empty (set empty if previously parsed as invalid).</p> <p>The severity of this vulnerability is lessened since an endpoint must be authenticated prior to reaching the crash point, or it's configured with no authentication.</p>
--------------------	--

Resolution	A stricter check is now done when pjproject retrieves the fmtmp attribute. Empty values are now properly handled.
-------------------	---

Affected Versions		
Product	Release Series	
Asterisk Open Source	13.x	All Releases
Asterisk Open Source	14.x	All Releases
Asterisk Open Source	15.x	All Releases
Certified Asterisk	13.18	All Releases

Asterisk Project Security Advisory - AST-2018-003

Copyright © 2018 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.

Asterisk Project Security Advisory - AST-2018-003

Corrected In	
Product	Release
Asterisk Open Source	13.19.2, 14.7.6, 15.2.2
Certified Asterisk	13.18-cert3

Patches	
SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2018-003-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2018-003-14.diff	Asterisk 14
http://downloads.asterisk.org/pub/security/AST-2018-003-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2018-003-13.18.diff	Certified Asterisk 13.18

Links	https://issues.asterisk.org/jira/browse/ASTERISK-27583
--------------	---

Asterisk Project Security Advisories are posted at <http://www.asterisk.org/security>
This document may be superseded by later versions; if so, the latest version will be posted at <http://downloads.digium.com/pub/security/AST-2018-003.pdf> and <http://downloads.digium.com/pub/security/AST-2018-003.html>

Revision History		
Date	Editor	Revisions Made
January 30, 2018	Kevin Harwell	Initial Revision
March 08, 2018	Kevin Harwell	Added CVE

Asterisk Project Security Advisory - AST-2018-003

Copyright © 2018 Digium, Inc. All Rights Reserved.

Permission is hereby granted to distribute and publish this advisory in its original, unaltered form.