

Asterisk Project Security Advisory - AST-2018-010

Product	Asterisk
Summary	Remote crash vulnerability DNS SRV and NAPTR lookups
Nature of Advisory	Denial Of Service
Susceptibility	Remote Unauthenticated Sessions
Severity	Moderate
Exploits Known	No
Reported On	October 23, 2018
Reported By	Jan Hoffmann
Posted On	November 14, 2018
Last Updated On	November 14, 2018
Advisory Contact	gjoseph AT digium DOT com
CVE Name	CVE-2018-19278

Description	There is a buffer overflow vulnerability in dns_srv and dns_naptr functions of Asterisk that allows an attacker to crash Asterisk via a specially crafted DNS SRV or NAPTR response. The attacker's request causes Asterisk to segfault and crash.
--------------------	--

Resolution	Upgrade Asterisk to a fixed version.
-------------------	--------------------------------------

Affected Versions		
Product	Release Series	
Asterisk Open Source	15.x	All releases
Asterisk Open Source	16.x	All releases

Corrected In	
Product	Release
Asterisk Open Source	15.6.2
Asterisk Open Source	16.0.1

Patches	
SVN URL	Revision

Asterisk Project Security Advisory - AST-2018-010

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-2018-010

http://downloads.asterisk.org/pub/security/AST-2018-010-15.diff	Asterisk 15
http://downloads.asterisk.org/pub/security/AST-2018-010-16.diff	Asterisk 16

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28127
--------------	---

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This document may be superseded by later versions; if so, the latest version will be posted at 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-2018-010.pdf> and <http://downloads.digium.com/pub/security/AST-2018-010.html>

Revision History		
Date	Editor	Revisions Made
October 25, 2018	George Joseph	Initial revision
November 14, 2018	George Joseph	Updated with CVE

Asterisk Project Security Advisory - AST-2018-010

Copyright © 2018 Digium, Inc. All Rights Reserved.

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