

Asterisk Project Security Advisory - AST-2021-006

Product	Asterisk
Summary	Crash when negotiating T.38 with a zero port
Nature of Advisory	Remote Crash
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	February 20, 2021
Reported By	Gregory Massel
Posted On	March 4, 2021
Last Updated On	March 4, 2021
Advisory Contact	bford AT sangoma DOT com
CVE Name	CVE-2019-15297

Description	When Asterisk sends a re-invite initiating T.38 faxing and the endpoint responds with a m=image line and zero port, a crash will occur in Asterisk. This is a reoccurrence of AST-2019-004.
Modules Affected	res_pjsip_t38.c

Resolution	<p>If T.38 faxing is not required then setting “t38_udptl” on the endpoint to “no” disables this functionality. This option is “no” by default.</p> <p>If T.38 faxing is required, then Asterisk should be upgraded to a fixed version.</p>
-------------------	---

Affected Versions		
Product	Release Series	
Asterisk Open Source	16.x	16.16.1
Asterisk Open Source	17.x	17.9.2
Asterisk Open Source	18.x	18.2.1
Certified Asterisk	16.x	16.8-cert6

Asterisk Project Security Advisory - AST-2021-006

Copyright © 02/25/2021 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-2021-006

Corrected In	
Product	Release
Asterisk Open Source	16.16.2, 17.9.3, 18.2.2
Certified Asterisk	16.8-cert7

Patches	
Patch URL	Revision
https://downloads.digium.com/pub/security/AST-2021-006-16.diff	Asterisk 16
https://downloads.digium.com/pub/security/AST-2021-006-17.diff	Asterisk 17
https://downloads.digium.com/pub/security/AST-2021-006-18.diff	Asterisk 18
https://downloads.digium.com/pub/security/AST-2021-006-16.8.diff	Certified Asterisk 16.8

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29203 https://downloads.asterisk.org/pub/security/AST-2021-006.html
--------------	--

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 This document may be superseded by later versions; if so, the latest version will be posted at <https://downloads.digium.com/pub/security/AST-2021-006.pdf> and <https://downloads.digium.com/pub/security/AST-2021-006.html>

Revision History		
Date	Editor	Revisions Made
February 25, 2021	Ben Ford	Initial revision
March 4, 2021	Ben Ford	Added 'posted on' date

Asterisk Project Security Advisory - AST-2021-006

Copyright © 02/25/2021 Digium, Inc. All Rights Reserved.

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