Product	Asterisk
Summary	Remote crash in res_pjsip_diversion
Nature of Advisory	Denial of service
Susceptibility	Remote authenticated sessions
Severity	Moderate
Exploits Known	Yes
Reported On	December 22, 2020
Reported By	Torrey Searle
Posted On	December 22, 2020
Last Updated On	December 23, 2020
Advisory Contact	kharwell AT sangoma DOT com
CVE Name	CVE-2020-35652

Description	A crash can occur in Asterisk when a SIP message is received that has a History-Info header, which contains a tel-uri. Note, the remote client must be authenticated, or Asterisk must be configured for anonymous calling in order for this problem to manifest.
Modules Affected	res_pjsip_diversion.c

Resolution	Asterisk now ensures that if it receives a SIP message with a History-Info header that contains a tel-uri the redirecting cause is simply set to unknown.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.X	13.38.0
Asterisk Open Source	16.X	16.15.0
Asterisk Open Source	17.X	17.9.0
Asterisk Open Source	18.X	18.1.0

Corrected In

Product	Release
Asterisk Open Source	13.38.1, 16.15.1, 17.9.1, 18.1.1

Patches

SVN URL	Revision
https://downloads.asterisk.org/pub/security/AST-2020-003-13.diff	Asterisk 13
https://downloads.asterisk.org/pub/security/AST-2020-003-16.diff	Asterisk 16
https://downloads.asterisk.org/pub/security/AST-2020-003-17.diff	Asterisk 17
https://downloads.asterisk.org/pub/security/AST-2020-003-18.diff	Asterisk 18

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29219

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2020-003.pdf and http://downloads.digium.com/pub/security/AST-2020-003.html

Revision History

Date	Editor	Revisions Made
December 22, 2020	Kevin Harwell	Initial revision
December 23. 2020	Kevin Harwell	Added CVE