Product	Asterisk
Summary	AMI user could execute system commands.
Nature of Advisory	Remote Code Execution
Susceptibility	Remote Authenticated Sessions
Severity	Minor
Exploits Known	No
Reported On	October 10, 2019
Reported By	Eliel Sardañons
Posted On	November 21, 2019
Last Updated On	November 21, 2019
Advisory Contact	gjoseph AT digium DOT com
CVE Name	CVE-2019-18610

Description	A remote authenticated Asterisk Manager Interface (AMI) user without "system" authorization could use a specially crafted "Originate" AMI request to execute arbitrary system commands.
Modules Affected	manager.c

Resolution	The specific parameters of the Originate AMI request that allowed the remote code execution are now blocked if the user does not have the "system" authorization.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	13.x	All releases
Asterisk Open Source	16.x	All releases
Asterisk Open Source	17.x	All releases
Certified Asterisk	13.21	All releases

Corrected In

Product	Release
Asterisk Open Source	13.29.2
Asterisk Open Source	16.6.2
Asterisk Open Source	17.0.1
Certified Asterisk	13.21-cert5

Patches

SVN URL	Revision
http://downloads.asterisk.org/pub/security/AST-2019-007-13.diff	Asterisk 13
http://downloads.asterisk.org/pub/security/AST-2019-007-16.diff	Asterisk 16
http://downloads.asterisk.org/pub/security/AST-2019-007-17.diff	Asterisk 17
http://downloads.asterisk.org/pub/security/AST-2019-007-13.21.diff	Certified Asterisk 13.21-cert5

Links	https://issues.asterisk.org/jira/browse/ASTERISK-28580

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This document may be superseded by later versions; if so, the latest version will be posted at http://downloads.digium.com/pub/security/AST-2019-007.pdf and http://downloads.digium.com/pub/security/AST-2019-007.html

Revision History

Date	Editor	Revisions Made
October 24, 2019	George Joseph	Initial Revision
November 21, 2019	Ben Ford	Added "Posted On" date