Product	Asterisk
Summary	pjproject: possible integer underflow on STUN message
Nature of Advisory	Arbitrary code execution
Susceptibility	Remote unauthenticated sessions
Severity	Major
Exploits Known	Yes
Reported On	March 3, 2022
Reported By	Sauw Ming
Posted On	March 4, 2022
Last Updated On	March 3, 2022
Advisory Contact	kharwell AT sangoma DOT com
CVE Name	CVE-2021-37706

Description	The header length on incoming STUN messages that contain an ERROR-CODE attribute is not properly checked. This can result in an integer underflow. Note, this requires ICE or WebRTC support to be in use with a malicious remote party.
Modules Affected	bundled pjproject

Resolution	If you use “with-pjproject-bundled” then upgrade to, or install one of, the versions of Asterisk listed below. Otherwise install the appropriate version of pjproject that contains the patch.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	16.x	All versions
Asterisk Open Source	18.x	All versions
Asterisk Open Source	19.x	All versions
Certified Asterisk	16.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	16.24.1,18.10.1,19.2.1
Certified Asterisk	16.8-cert13

Patches	
Patch URL	**Revision**
https://downloads.digium.com/pub/security/AST-2022-004-16.diff	Asterisk 16
https://downloads.digium.com/pub/security/AST-2022-004-18.diff	Asterisk 18
https://downloads.digium.com/pub/security/AST-2022-004-19.diff	Asterisk 19
https://downloads.digium.com/pub/security/AST-2022-004-16.8.diff	Certified Asterisk 16.8

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29945 https://downloads.asterisk.org/pub/security/AST-2022-004.html https://github.com/pjsip/pjproject/security/advisories/GHSA-2qpg-f6wf-w984

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This document may be superseded by later versions; if so, the latest version will be posted at https://downloads.digium.com/pub/security/AST-2022-004.pdf and https://downloads.digium.com/pub/security/AST-2022-004.html

Revision History		
Date	**Editor**	**Revisions Made**
March 3, 2022	Kevin Harwell	Initial revision