Product	Asterisk
Summary	res_stir_shaken: SSRF vulnerability with Identity header
Nature of Advisory	Server-side request forgery
Susceptibility	Remote unauthenticated access
Severity	Major
Exploits Known	No
Reported On	Jun 10, 2021
Reported By	Clint Ruoho
Posted On	Apr 14, 2022
Last Updated On	April 13, 2022
Advisory Contact	bford AT sangoma DOT com
CVE Name	CVE-2022-26499

Description	When using STIR/SHAKEN, it’s possible to send arbitrary requests like GET to interfaces such as localhost using the Identity header.
Modules Affected	res_stir_shaken

Resolution	If you are using STIR/SHAKEN in Asterisk, upgrade to one of the versions listed below to get a new configuration option: stir_shaken_profile. This can be configured in stir_shaken.conf and set on a per endpoint basis in pjsip.conf. This option will take priority over the stir_shaken option. The stir_shaken_profile will contain the stir_shaken option (attest, verify, or both), as well as ACL configuration options to permit and deny specific IP addresses / hosts. The ACL will be used for the public key URL we receive in the Identity header, which is used to tell Asterisk where to download the public certificate. An ACL from acl.conf can be used, but you can specify your own permit and deny lines within the profile itself. A combination of both can also be used. Note that this patch contains changes that affect the same area as the patch from AST-2022-001. It is recommended that you upgrade to a listed version, otherwise you might encounter merge conflicts.

Affected Versions		
Product	**Release Series**	
Asterisk Open Source	16.x	16.15.0 and after
Asterisk Open Source	18.x	All versions
Asterisk Open Source	19.x	All versions

Corrected In	
Product	**Release**
Asterisk Open Source	16.25.2, 18.11.2, 19.3.2

Patches	
Patch URL	**Revision**
https://downloads.digium.com/pub/security/AST-2022-002-16.diff	Asterisk 16
https://downloads.digium.com/pub/security/AST-2022-002-18.diff	Asterisk 18
https://downloads.digium.com/pub/security/AST-2022-002-19.diff	Asterisk 19

Links	https://issues.asterisk.org/jira/browse/ASTERISK-29476 https://downloads.asterisk.org/pub/security/AST-2022-002.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This document may be superseded by later versions; if so, the latest version will be posted at https://downloads.digium.com/pub/security/AST-2022-002.pdf and https://downloads.digium.com/pub/security/AST-2022-002.html

Revision History		
Date	**Editor**	**Revisions Made**
Apr 13, 2022	Ben Ford	Initial revision