

## Asterisk Project Security Advisory - AST-2022-001

<b>Product</b>	Asterisk
<b>Summary</b>	res_stir_shaken: resource exhaustion with large files
<b>Nature of Advisory</b>	Resource exhaustion
<b>Susceptibility</b>	Remote unauthenticated access
<b>Severity</b>	Major
<b>Exploits Known</b>	No
<b>Reported On</b>	Jan 21, 2022
<b>Reported By</b>	Ben Ford
<b>Posted On</b>	Apr 14, 2022
<b>Last Updated On</b>	April 13, 2022
<b>Advisory Contact</b>	bford AT sangoma DOT com
<b>CVE Name</b>	CVE-2022-26498

<b>Description</b>	When using STIR/SHAKEN, it's possible to download files that are not certificates. These files could be much larger than what you would expect to download.
<b>Modules Affected</b>	res_stir_shaken

<b>Resolution</b>	<p>If you are using STIR/SHAKEN in Asterisk, upgrade to one of the versions listed below. Asterisk now checks the downloaded file to see if it's actually a certificate or if it is larger than what is expected.</p> <p>If not upgrading, the curl_timeout option in stir_shaken.conf should be utilized so that downloads do not last an extended period of time.</p>
-------------------	---

<b>Affected Versions</b>		
<b>Product</b>	<b>Release Series</b>	
Asterisk Open Source	16.x	16.15.0 and after
Asterisk Open Source	18.x	All versions
Asterisk Open Source	19.x	All versions

## Asterisk Project Security Advisory - AST-2022-001

Copyright © 01/19/2022 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-2022-001

<b>Corrected In</b>	
<b>Product</b>	<b>Release</b>
Asterisk Open Source	16.25.2, 18.11.2, 19.3.2

<b>Patches</b>	
<b>Patch URL</b>	<b>Revision</b>
<a href="https://downloads.digium.com/pub/security/AST-2022-001-16.diff">https://downloads.digium.com/pub/security/AST-2022-001-16.diff</a>	Asterisk 16
<a href="https://downloads.digium.com/pub/security/AST-2022-001-18.diff">https://downloads.digium.com/pub/security/AST-2022-001-18.diff</a>	Asterisk 18
<a href="https://downloads.digium.com/pub/security/AST-2022-001-19.diff">https://downloads.digium.com/pub/security/AST-2022-001-19.diff</a>	Asterisk 19

<b>Links</b>	<a href="https://issues.asterisk.org/jira/browse/ASTERISK-29872">https://issues.asterisk.org/jira/browse/ASTERISK-29872</a> <a href="https://downloads.asterisk.org/pub/security/AST-2022-001.html">https://downloads.asterisk.org/pub/security/AST-2022-001.html</a>
--------------	--

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-2022-001.pdf> and <https://downloads.digium.com/pub/security/AST-2022-001.html>

<b>Revision History</b>		
<b>Date</b>	<b>Editor</b>	<b>Revisions Made</b>
Apr 13, 2022	Ben Ford	Initial revision

Asterisk Project Security Advisory - AST-2022-001

Copyright © 01/19/2022 Digium, Inc. All Rights Reserved.

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