| | |
|---|---|
| **Product** | Asterisk |
| **Summary** | BEAST vulnerability in HTTP server |
| **Nature of Advisory** | Unauthorized data disclosure due to man-in-the-middle attack |
| **Susceptibility** | Remote unauthenticated sessions |
| **Severity** | Minor |
| **Exploits Known** | Yes |
| **Reported On** | 04/15/15 |
| **Reported By** | Alex A. Welzl |
| **Posted On** | 02/03/16 |
| **Last Updated On** | February 15, 2016 |
| **Advisory Contact** | Joshua Colp <jcolp AT digium DOT com> |
| **CVE Name** | CVE-2011-3389 |

| | |
|---|---|
| **Description** | The Asterisk HTTP server currently has a default configuration which allows the BEAST vulnerability to be exploited if the TLS functionality is enabled. This can allow a man-in-the-middle attack to decrypt data passing through it. |

| | |
|---|---|
| **Resolution** | Additional configuration options have been added to Asterisk which allow configuration of the HTTP server to not be susceptible to the BEAST vulnerability. These include options to confirm the permitted ciphers, to control what TLS protocols are allowed, and to use server cipher preference order instead of client preference order. The default configuration has also been changed for the HTTP server to use a configuration which is not susceptible to the BEAST vulnerability. |

| **Affected Versions** | | |
|---|---|---|
| **Product** | **Release Series** | |
| Asterisk Open Source | 1.8.x | All Versions |
| Asterisk Open Source | 11.x | All Versions |
| Asterisk Open Source | 12.x | All Versions |
| Asterisk Open Source | 13.x | All Versions |
| Certified Asterisk | 1.8.28 | All Versions |
| Certified Asterisk | 11.6 | All Versions |
| Certified Asterisk | 13.1 | All Versions |

| Corrected In | |
|---|---|
| **Product** | **Release** |
| Asterisk Open Source | 11.21.1, 13.7.1 |
| Certified Asterisk | 11.6-cert12, 13.1-cert3 |

| Patches | |
|---|---|
| **SVN URL** | **Revision** |
| http://downloads.asterisk.org/pub/security/AST-2016-001-1.8.28.diff | Certified Asterisk 1.8.28 |
| http://downloads.asterisk.org/pub/security/AST-2016-001-11.6.diff | Certified Asterisk 11.6 |
| http://downloads.asterisk.org/pub/security/AST-2016-001-13.1.diff | Certified Asterisk 13.1 |
| http://downloads.asterisk.org/pub/security/AST-2016-001-11.diff | Asterisk 11 |
| http://downloads.asterisk.org/pub/security/AST-2016-001-12.diff | Asterisk 12 |
| http://downloads.asterisk.org/pub/security/AST-2016-001-13.diff | Asterisk 13 |

| **Links** | https://issues.asterisk.org/jira/browse/ASTERISK-24972 |
|---|---|

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-2016-001.pdf and http://downloads.digium.com/pub/security/AST-2016-001.html

| Revision History | | |
|---|---|---|
| **Date** | **Editor** | **Revisions Made** |
| 3 August, 2015 | Joshua Colp | Initial creation of document |
| 15 February 2016 | Kevin Harwell | CVE assignment |