Security

This page exists to provide quick reference to all past security notices that affect SpamAssassin. At this time this page is a work-in-progress, but it is believed to be complete.

Please note that while this reference does cover security notices for versions of SpamAssassin prior to version 3.0.0, it should be noted these are pre-Apache releases. They are included here for completeness. Also note this document does not attempt to cover versions older than 2.40.

Please also note that these notices apply to the official releases of SpamAssassin. Some third party distribution packages, such as Debian, choose to backport fixes. If you are using a distribution package with a version that appears vulnerable, check with the security advisories for that distribution to see if the fix has been backported.

Security Items Fixed with SpamAssassin 3.4.2
[CVEID]:CVE-2017-15705
[PRODUCT]:Apache SpamAssassin
[VERSION]:Apache SpamAssassin 1.5 to 3.4.1
[PROBLEMTYPE]:Denial of Service
[REFERENCES]:https://lists.apache.org/thread.html/7f6a16bc0fd0fd5e67c7fd95bd655069a2ac7d1f88e42d3c853e601c@%3Cannounce.apache.org%3E
[DESCRIPTION]:While working on bug 7437, a denial of service vulnerability was identified that exists in all modern versions of Apache SpamAssassin.

The vulnerability arises with certain unclosed tags in emails that cause markup to be handled incorrectly leading to scan timeouts.

In Apache SpamAssassin, using HTML::Parser, we setup an object and hook into the begin and end tag event handlers In both cases, the "open" event is immediately followed by a "close" event - even if the tag *does not* close in the HTML being parsed.

Because of this, we are missing the "text" event to deal with the object normally. This can cause carefully crafted emails that might take more scan time than expected leading to a Denial of Service.

The issue is possibly a bug or design decision in HTML::Parser that specifically impacts the way Apache SpamAssassin uses the module with poorly formed html.

The exploit has been seen in the wild but not believed to have been purposefully part of a Denial of Service attempt. We are concerned that there may be attempts to abuse the vulnerability in the future. Therefore, we strongly recommend all users of these versions upgrade to Apache SpamAssassin 3.4.2 as soon as possible.

[CVEID]:CVE-2016-1238
[PRODUCT]:Apache SpamAssassin
[VERSION]:Apache SpamAssassin 1.5 to 3.4.1
[PROBLEMTYPE]:Unsafe Include Path
[REFERENCES]:https://lists.apache.org/thread.html/7f6a16bc0fd0fd5e67c7fd95bd655069a2ac7d1f88e42d3c853e601c@%3Cannounce.apache.org%3E
[DESCRIPTION]:While working on bug 7378, an issue that might allow improper code to be purposefully or accidentally included was identiied. This release also fixes a reliance on "." in @INC in one configuration script. Whether this can be exploited in any way is uncertain.

[CVEID]:CVE-2018-11780
[PRODUCT]:Apache SpamAssassin
[VERSION]:Apache SpamAssassin 3.4.1
[PROBLEMTYPE]:Remote Code Execution
[REFERENCES]:https://lists.apache.org/thread.html/7f6a16bc0fd0fd5e67c7fd95bd655069a2ac7d1f88e42d3c853e601c@%3Cannounce.apache.org%3E
[DESCRIPTION]:While working on bug 7556, we identified a potential Remote Code Execution bug with the PDFInfo plugin. Thanks to cPanel Security Team for their report of this issue. This issue only exists in Apache SpamAssassin 3.4.1 and newer and the plugin is not enabled by default.

[CVEID]:CVE-2018-11781
[PRODUCT]:Apache SpamAssassin
[VERSION]:Apache SpamAssassin 3.1.0 to 3.4.1
[PROBLEMTYPE]:Local Code Execution
[REFERENCES]:https://lists.apache.org/thread.html/7f6a16bc0fd0fd5e67c7fd95bd655069a2ac7d1f88e42d3c853e601c@%3Cannounce.apache.org%3E
[DESCRIPTION]:While working on bug 7557, this release fixes a local user code injection in the meta rule syntax. Thanks again to cPanel Security Team for their report of this issue. This issue affects SpamAssassin 3.1.0 to 3.4.1. Upgrading to 3.4.2 is highly recommended though it is believed this is only exploitable with unsafe external rules loaded by an admin or with local users and allow_user_rules enabled.

Previous Security Issues

Local user symlink-attack DoS vulnerability with "spamd --allow-tell -x" and other options

Versions affected: 3.1.0-3.1.8, 3.2.0

Fixed in: 3.1.9, 3.2.1

References:
http://spamassassin.apache.org/advisories/cve-2007-2873.txt http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2873

Overly long URLs DoS

Versions affected: 3.1.0-3.1.7

Fixed in: 3.1.8

References:
http://spamassassin.apache.org/advisories/cve-2007-0451.txt http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0451

spamd remote code execution if -v AND -P options used

Versions affected: 2.50-3.0.5, 3.1.0-3.1.2

Fixed in: 3.0.6, 3.1.3

References:
http://spamassassin.apache.org/advisories/cve-2006-2447.txt http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2447

"many To: headers" DoS vuln

Versions affected: 3.0.4, possibly older versions.

Fixed in: 3.0.5, 3.1.0

References:
http://secunia.com/advisories/17386/ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3351

malformed message with long headers DoS

Versions affected: 3.0.1-3.0.3

Fixed in: 3.0.4

References:
http://secunia.com/advisories/15704/ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1266

Unspecified malformed message DoS

Versions affected: 2.50-2.63 (pre-Apache releases)

Fixed in: 2.64

References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0796

Arbitrary code execution if BSMTP used

Versions affected: 2.40-2.43 (pre-Apache releases)

Fixed in: 2.44

References:
http://www.securityfocus.com/bid/6679 http://secunia.com/advisories/7951/