

[VulnWatch] bogofilter-SA-2004-01: RFC 2047 Denial-of-service in 0.17.4 <= bogofilter <= 0.92.7

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-10/0017.html>

From: Matthias Andree (matthias.andree_at_gmx.de)

Date: 10/30/04

Date: Sat, 30 Oct 2004 15:22:27 +0200

To: bugtraq@securityfocus.com, full-disclosure@lists.netsys.com, vulnwatch@vulnwatch.org, bogofilter@vulnwatch.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

bogofilter-SA-2004-01 rfc2047crash

Topic: vulnerability in bogofilter/bogolexer

Announcement: bogofilter-SA-2004-01

Writer: Matthias Andree

Version: 1.00

CVE id: (none yet)

Announced: 2004-10-30

Category: vulnerability

Type: segmentation fault through malformed input

Impact: denial of service

Credits: Antti-Juhani Kaijanaho, Clint Adams, David Relson

Danger: medium

URL: <http://bogofilter.sourceforge.net/security/bogofilter-SA-2004-01>

Affected: bogofilter (stable) 0.92.6, 0.92.4, 0.92.0, 0.17.5

 bogofilter (current) 0.17.4 to 0.92.7 (inclusive)

Not affected: bogofilter 0.17.3 and older

 bogofilter 0.92.8 and newer

Introduced: 2004-03-20 21:46:39 UTC (CVS)

 2004-03-20 22:20 bogofilter 0.17.4 released as current

 2004-04-02 01:00 bogofilter 0.17.5 released as stable

Corrected: 2004-10-08 23:50:04 UTC (CVS) – committed corrected version

 2004-10-25 bogofilter 0.92.8 released as stable

 2004-10-26 recognized bug as a vulnerability

References: Debian Bug #275373

 FreeBSD VuXML ID f4428842-a583-4a4c-89b7-297c3459a1c3

FreeBSD Problem Report #73144

0. Release history

2004-10-28 0.01 initial draft for internal review
2004-10-30 0.02 minor revision, added URL
2004-10-30 1.00 minor revision by David Relson, published.

1. Background

Bogofilter is a software package to classify a mail as spam or non-spam. It uses a data base to store words and must be trained which mail are spam and non-spam. It uses the probabilities of individual words for classifying the message.

Bogofilter understands enough of MIME to decode headers and only consider text parts of mail.

2. Problem description

Antti-Juhani Kaijanaho provided Debian with a test case that crashed bogofilter 0.92.7. The problem was examined and tracked down to a change in bogofilter's quoted-printable decoder that went into 0.17.4.

The pertinent change allowed the quoted-printable decoder to accept LF in encoded words but replaced it by a NUL character, which the calling function inside bogofilter could not handle. It attempted to write a NUL byte either one byte past the end of a buffer provided by the lexical analyzer or to an address that was the negative of the address of the first byte of the "encoded text" part of the encoded word that was supposed to be decoded.

It was decided to announce this as a vulnerability because bogofilter cannot process the pertinent message.

3. Impact

This vulnerability causes bogofilter to catch a "segmentation violation" signal, which causes an immediate program abort.

The exact impact depends on the way bogofilter is integrated into the system. In common setups, the mail that contains such malformed headers is deferred by the mail delivery agent and remains in the queue, where it will eventually bounce back to the sender.

4. Workaround

No reasonable workaround is known at this time.

5. Solution

VulnWatch: [VulnWatch] bogofilter-SA-2004-01: RFC 2047 Denial-of-service in 0.17.4 <= bogofilter <= 0.92.7

Upgrade your bogofilter to version 0.92.8.

bogofilter 0.92.8 is available from sourceforge:

http://sourceforge.net/project/showfiles.php?group_id=62265&package_id=59357&release_id=277823

Note that a broken-out bugfix patch is not available at this time, because the reversion of the failure-inducing change is not a complete fix. Besides, bogofilter is under development and support is limited to the latest available "current" plus the latest available "stable" versions.

END of bogofilter-SA-2004-01 rfc2047crash

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (GNU/Linux)

iD8DBQFBg5WTvmGDOQUufZURAIL5AKCm5BhqXeDzayXQ69qL6SOQcyKikgCfWH1a

ZzR2ULmqEV/INwBjZLkz9Hc=

=eSc6

-----END PGP SIGNATURE-----

[VulnWatch] bogofilter-SA-2004-01: RFC 2047 Denial-of-service in 0.17.4 <= bogofilter <= 0.92.7