

[NEWS] Multiple Vendor Long ZIP Entry Filename Processing Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0014.html>

From: support@securiteam.com

Date: 10/03/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 3 Oct 2002 23:55:43 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Multiple Vendor Long ZIP Entry Filename Processing Issues

SUMMARY

Products and libraries from multiple vendors are deficient in their handling of zip files having entries with long filenames. Typically, opening and/or processing these crafted zip files will result in the program crashing or exhibiting unpredictable behavior. There is a possibility of arbitrary code execution, but no exploits are known at this time.

DETAILS

Affected system(s):

Several different vendors and products were tested. Many were found to be vulnerable. A partial list of affected vendors follows.

Detailed results for many vendors are being withheld pending their response to the issues described in this advisory. We encourage customers to engage your vendors on this issue if you have any questions regarding their handling of specially crafted ZIP files.

For an up-to-date list of vendor statements, see CERT Vulnerability Note VU#383779.

Securiteam: [NEWS] Multiple Vendor Long ZIP Entry Filename Processing Issues

Known vulnerable:

- o Microsoft Windows XP
- o Microsoft Windows ME
- o Microsoft Windows 98 With Plus! Pack
- o Lotus Notes R4
- o Lotus Notes R5
- o Lotus Notes R6 (pre-gold)
- o Verity, Inc. KeyView viewing SDK
- o Aladdin Systems Stuffit Expander (pre 7.0)

Apparently not vulnerable:

- o WinRAR is believed to be NOT vulnerable
- o WinZip 8.x is believed to be NOT vulnerable
- o zlib is believed to be NOT vulnerable

Vendor status and information:

This is a partial list of affected products and vendors. We will update our advisory as we get feedback from more vendors. You may check back with us at: <<http://www.rapid7.com/SecurityResearch.html>>
<http://www.rapid7.com/SecurityResearch.html>.

Microsoft Windows XP

Explorer.exe crashes when navigating through specially crafted ZIP files.

The shell (Explorer.exe) in Windows XP provides functionality to uncompress ZIP files on-the-fly, and presents them as folders that users can navigate through. There exists a buffer overflow in this feature which may allow malicious ZIP files to be constructed that execute code upon access. It should be noted that Explorer.exe does not display the filename if it is too long. This may work to an attacker's advantage since suspicious filenames would be hidden from the user.

Microsoft was notified of this issue, and a fix is available. More information can be found in Microsoft Security Advisory MS02-054. This issue has been assigned a CVE ID of CAN-2002-0370.

Microsoft Windows ME

Windows ME provides functionality to uncompress ZIP files on-the-fly, and presents them as folders that users can navigate through. There exists a buffer overflow in this feature which may allow malicious ZIP files to be constructed that execute code upon access.

Microsoft was notified of this issue, and a fix is available. More information can be found in Microsoft Security Advisory MS02-054. This issue has been assigned a CVE ID of CAN-2002-0370.

Microsoft Windows 98 With Plus! Pack

Windows 98 provides functionality to uncompress ZIP files on-the-fly, and presents them as folders that users can navigate through. There exists a buffer overflow in this feature which may allow malicious ZIP files to be constructed that execute code upon access.

Securiteam: [NEWS] Multiple Vendor Long ZIP Entry Filename Processing Issues

Microsoft was notified of this issue, and a fix is available. More information can be found in Microsoft Security Advisory MS02-054. This issue has been assigned a CVE ID of CAN-2002-0370.

Lotus Notes Client R4

Lotus Notes Client R5 and R6 (pre-gold)

Lotus Notes Client R4 crashes when viewing certain zip files using the built-in attachment viewer.

The R4 Lotus Notes client incorporated attachment viewer technology licensed from a third party. Choosing "View" attachment will invoke the viewer, which causes the Lotus Notes client to crash.

Lotus has been contacted regarding this issue. Fix information is unknown. Newer clients (R5 and R6) bundle a different attachment viewer (see below), which is also vulnerable.

This issue is being tracked as SPR# KSPR5CJV2G.

Lotus Notes R5.0.11 and earlier are vulnerable. Lotus plans to fix this issue in the next maintenance release of R5.

All pre-Gold versions of Lotus Notes R6 are vulnerable. Lotus has included the fix in R6 Gold and higher.

Verity KeyView viewing SDK

Products based on Verity, Inc.'s KeyView SDK may crash on specially crafted files.

Verity has been contacted regarding this issue. Verity has produced a fix to SDK v7.0 which is available to SDK customers via Verity technical support. They are tracking this as bug number 76316.

Since the Verity SDK is licensed by many different vendors, concerned customers should obtain a fix directly from their vendor, rather than contacting Verity directly.

Aladdin Stuffit Expander (all platforms)

Aladdin Stuffit Expander versions prior to 7.0 may crash on specially crafted zip files.

Aladdin Systems, Inc. has been contacted regarding this issue. Newer versions of Stuffit Expander are believed NOT to be vulnerable. Please see <http://www.stuffit.com/expander/cert.html> for upgrade instructions and more information.

Solution:

Obtain a fix from your vendor.

Securiteam: [NEWS] Multiple Vendor Long ZIP Entry Filename Processing Issues

Detailed analysis:

The ZIP file format reserves two bytes to indicate the length of an entry filename, which allows entry names of up to 65,535 characters.

Many vendors have been tested and notified. Many products whose primary purpose has nothing to do with compression contain ZIP processing functionality for one reason or another. Some examples include virus scanners, content scanning email gateways, "skinnable" products whose skins are packaged in the ZIP format, and so on.

The original Info-ZIP public domain source code and its derivatives (zlib, etc.) do not appear to be vulnerable. However, we noticed crashes in several Info-ZIP derived products — the crashes typically occurred in the user interface code, rather than the core ZIP processing routines.

To facilitate testing efforts by vendors and customers, we have made several example ZIP files available on our website. Anyone may download these files from <http://www.rapid7.com/SecurityResearch.html> after agreeing to Rapid7's terms of use.

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@rapid7.com> Rapid 7 Security Advisories.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Flood of ACK Packets Cause AIX DoS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)