Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability

ReversingLabs Corporation - Security Advisory

I. BACKGROUND

This vulnerability affects multiple anti-virus vendors including Eset, Panda, Norman, Sophos, Symantec, Sunbelt, TrendMicro, VirusBuster, F-Prot, Fortinet and Ikarus.

II. FORMAT BACKGROUND

ZIP file format is one of the most common archive file formats used today. The format was originally created in 1986 by Phil Katz for PKZIP, and evolved from the previous ARC compression format by Thom Henderson. The PKZIP format is now supported by many software utilities other than PKZIP (see List of file archivers). Microsoft has included built-in ZIP support (under the name "compressed folders") in versions of its Windows operating system since 1998. Apple has included built-in ZIP support in Mac OS X 10.3 and later.

ZIP is a simple archive format that compresses every file separately. Compressing files separately allows for individual files to be retrieved without reading through other data; in theory, it may allow better compression by using different algorithms for different files. A caveat to this is that archives containing a large number of small files end up significantly larger than if they were compressed as a single file, due to the fact that the data structures which store information on each individual file are stored uncompressed.

The ZIP file contents are files and directories which are stored in arbitrary order. The location of a file is indicated in a section called the “central directory,” located at the end of the ZIP file. The files and directories are represented by “file entries.”

Each file entry is introduced by a local header with information about the file such as a comment, file size and file name, followed by optional "extra" data fields, and then the file data which may be compressed, encrypted, or both. The "extra" data fields are the key to the extensibility of the ZIP format. These fields are used to provide support for ZIP64 formats, WinZip-compatible AES encryption, and NTFS file timestamps. In theory, many other extensions are possible via the coded "extra" fields.

The central directory consists of file headers holding, among other metadata, the file name and the relative offset in the archive of the local header for each file entry. Each file entry is marked by a specific 4-byte "signature"; each entry in the central directory is likewise marked with its own particular 4-byte signature. ZIP file parsers typically look for the appropriate signature when parsing a ZIP file. Since the order of file entries in the directory need not conform to the order of file entries in the archive, the format is non-sequential. There is no BOF or EOF marker in the ZIP spec. Instead, ZIP tools scan for the signatures of the various fields.

There are numerous ZIP tools available, and numerous ZIP libraries for various programming environments. Some of the libraries are commercial, some are not. Some are open source, some are not. WinZip is perhaps the most popular and famous - it runs primarily on Windows, enabling end users to create or extract ZIP files. WinRAR, IZarc, Info-zip, 7-zip are other tools, available on various platforms. Some of those tools have library or programmatic interfaces.

III. DESCRIPTION

The remote exploitation of an “exceptional condition” error in multiple anti-virus software packages allows attackers to bypass security protections by evading virus detection. A special kind of ZIP header malformation enables virus writers to evade malware detection by the listed antivirus vendors. This kind of malformation can also be used to introduce steganographic[1] content into existing ZIP achieves.

In order to craft such a file we must damage the header in such way that these programs will be forced to skip over the packed file,without detecting any information about the damage, so they will work normally with the archive. This can be done in number of ways. The following procedure describes one method:

1) Reset ZIPCentralEntry.InternalFileAttributes to NULL
2) Move the first character of the name to ZIPCentralEntry.InternalFileAttributes
3) Set the first character of the name to NULL
4) Set the ZIPCentralEntry. ExternalFileAttributes to ZIPCentralEntry. RelativeOffsetOfLocalHeader
5) Reset the two bytes pointed to by ZIPCentralEntry. RelativeOffsetOfLocalHeader to NULL
6) Reset ZIPCentralEntry. RelativeOffsetOfLocalHeader to NULL

This overwrites the file attributes with no chance of their restoration. However, the default value for file attributes is 0x20 which means that the file is an archive, which is why we set those fields to that value when reversing the procedure. The only limitation to using this hiding technique is that the first file in the archive can’t be hidden because it is used as an anchor for the files that are packed after it.

However if the first file in the archive is hidden via the procedure described above, vulnerable antivirus vendors stop scanning at the first file, and don’t check the rest of the archive. Despite this file modification, all the programs that work with ZIP file format (*such as WinZIP, WinRAR, 7ZIP, PowerArchiver and Compressed Folders that comes with Windows*) had no problems extracting or testing the integrity of the corrupted archives.

[1] *“Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means concealed writing.”*

IV. TESTING

Scanning of specially crafted files by the technique described above has been performed by the website: www.virustotal.com

Scanning results are available in the archive:

- **VTotal-NormalArchive.pdf**; Normally compressed ZBOT malware sample inside a valid ZIP archive.
- **VTotal-ZipMod2.pdf**; After creating a normal ZIP archive which packs a single text file and a ZBOT sample we malformed the header so that the text file is hidden (as described above) and the malware is visible. Since first file in the header is hidden and considered broken many of the antivirus products stop their scan there.
- **VTotal-Zipx**; Normally compressed ZBOT malware sample inside a valid ZIPX archive.

V. WORKAROUND

Filter all compressed file archives (.zip) at border gateways, regardless of content and damaged headers.

VI. VENDOR RESPONSES

- Waiting for response -

VIII. DISCLOSURE TIMELINE

- January 2010; Initial vendor notification
- April 12, 2010; Public disclosure at Black Hat Barcelona 2010

IX. CREDITS

This vulnerability was discovered by employees of ReversingLabs Corporation.

X. LEGAL NOTICES

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.