Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability

ReversingLabs Corporation - Security Advisory

I. BACKGROUND

This vulnerability affects multiple anti-virus vendors including AVG, DrWeb, Fortinet, Ikarus, Kaspersky, Rising and Symantec.

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. Detection evasion is achieved by appending a simple ZIP archive, containing a malicious sample, to the end of the self-extractor module. In order to fool programs that work with ZIP archives the appended file is aligned to its appended offset, making it behave like a valid archive which can be extracted by all programs that work with ZIP format. However, even though a ZIP file is appended to the end of the self-extractor module, the original content is still extracted when the SFX is executed. This happens because the SFX module stores compressed data in the last portable executable section and extracts from there.

IV. TESTING

Scanning of packed files by the technique described above has been performed by the website: www.virustotal.com, Scanning results are available in the archive:

- **VTotal-ZIPSFX.pdf**; ZIP SFX compressed Conficker sample.
- **VTotal-ZIPSFX-OVL-OLD.pdf**; Conficker packed inside the ZIP SFX archive on which another ZIP file is appended.
- **VTotal-ZIPSFX-OVL-NEW.pdf**; Conficker packed inside the ZIP SFX archive on which another ZIP file is appended.

V. WORKAROUND

Filter all compressed file self extracting archives (.exe) at border gateways, processing the whole content, 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.

ReversingLabs Corporation

X. LEGAL NOTICES