

[NT] Apple iTunes Playlist Parsing Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/16/05

To: list@securiteam.com

Date: 16 Jan 2005 10:59:00 +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>

Apple iTunes Playlist Parsing Buffer Overflow

SUMMARY

<<http://www.apple.com/itunes/>> Apple iTunes is "a digital jukebox capable of playing a variety of sound file formats, sharing music and burning music CD's". Remote exploitation of a buffer overflow vulnerability in Apple Computer Inc.'s iTunes music player allows attackers to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Apple iTunes version 4.7 and prior

Immune Systems:

- * Apple iTunes version 4.7.1 or newer

The problem specifically exists when parsing playlist files that contain long URL file entries. Malicious playlist files can come with either the m3u or .pls extension. Though their formats are different, the vulnerability in each is the same.

An example malicious .pls file with a long URL:

[playlist]

Securiteam: [NT] Apple iTunes Playlist Parsing Buffer Overflow

NumberOfEntries=1
File1=http://[A x 3045]1234

An example malicious .m3u file with a long URL:
http://[A x 3045]1234

In both cases '[A x 3045]' represents any string of 3,045 bytes in length. Opening either malicious playlist file on the Microsoft Windows platform will cause iTunes to crash with an access violation when attempting to execute instruction 0x34333231, which is the little-endian ASCII code representation of '1234'. An attacker can exploit this vulnerability to redirect the flow of control and eventually execute arbitrary code. While this example is specific to the Microsoft Windows platform, exploitation on the Apple Mac OS platform is also possible.

Analysis:

Exploitation of the described vulnerability allows remote attackers to execute arbitrary code under the context of the user who started iTunes. Exploitation requires that an attacker convince a target user to open a malicious playlist file with a vulnerable version of iTunes.

Workaround:

Do not open playlist files from untrusted sources. Inspect the contents of m3u and .pls playlist files for long URL file names prior to opening them with iTunes.

Vendor response:

This vulnerability is addressed in iTunes 4.7.1. iTunes 4.7.1 may be obtained from the Software Update pane in System Preferences, or Apple's iTunes download site: <<http://www.apple.com/itunes/download/>>
<http://www.apple.com/itunes/download/>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0043>>
CAN-2005-0043

Disclosure Timeline:

12/17/2004 – Initial vendor notification
12/17/2004 – Initial vendor response
01/13/2004 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> IDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=180&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=180&type=vulnerabilities>

=====

Securiteam: [NT] Apple iTunes Playlist Parsing Buffer Overflow

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.