security-assessment.com

Vulnerability Advisory

Name	Winamp - Buffer Overflow In IN_CDDA.dll
Vendor Update	http://www.winamp.com/player/
Date Released	November 23, 2004
Affected Software	Winamp 5.06, 5.05 and others below
Researcher	Brett Moore brett.moore@security-assessment.com

Description

We discovered a remotely exploitable stack based buffer overflow in winamp version 5.05. It is possible that earlier versions are also vulnerable and we recommend all users to upgrade to the latest version.

The overflow can be caused in various ways, the most dangerous though is through a malformed .m3u playlist file. When hosted on a web site, these files will be automatically downloaded and opened in winamp without any user interaction. This is enough to cause the overflow that would allow a malicious playlist to overwrite EIP and execute arbitrary code.

Exploitation

When winamp opens the malformed playlist file, a first exception will occur:

First Chance Exception in winamp.exe (IN_CDDA.DLL) : Access Violation
At this location
00A49BE8 88 4C 04 30 mov byte ptr [esp+eax+30h],cl

This exception will be handled by winamp, and execution will then continue until it reaches the second exception at this location
61616161 ???

with the registers looking like;
EAX = 0012A5D8 EBX = 0012C024
ECX = 61616161 EDX = 77F96DAE
ESI = 0012A600 EDI = 0046B9E0
EIP = 61616161 ESP = 0012A540
EBP = 0012A560 EFL = 00210246

As can be seen, EIP has been overwritten with a value supplied through the malformed playlist file, 0x61616161 (aaaa) and since more playlist supplied data is located at the address pointed to by EDI, execution of malicious code is possible.

Solution

It has been discovered that the initial patch by the vendor did not correctly address this issue.
It is recommended that the .m3u and .cda extensions are disassociated with the winamp player.
Check the vendor website for updates. **http://www.winamp.com/player/**

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and our team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093