



Vulnerability Advisory

Name	VideoLAN VLC Memory Corruption
Vendor Website	http://www.videolan.org/
Date Released	07/04/2014
Affected Software	VideoLAN VLC Media Player
Researchers	Scott Bell

Description

VideoLAN VLC Media player is affected by a memory corruption vulnerability which can potentially allow a remote attacker to compromise a victim's machine.

Exploitation

Exploitation of this vulnerability requires a user to open a malicious video file. Users can generally be lured to visit to open video files via email, instant message or links on the Internet. Vulnerabilities like this are often hosted on legitimate websites which have been compromised by other means. The following MP4 file can be used to reproduce the vulnerability:

Proof of Concept

<https://trac.videolan.org/vlc/attachment/ticket/11162/test.mp4>

Solution

A fix for this vulnerability was landed with the following commit:

<http://git.videolan.org/gitweb.cgi/vlc.git/?a=commit;h=7c82aac1267eccf02ec7306d5aa0fb76e8b873a4>

Security-Assessment.com recommends updating to the latest version provided by the vendor. For more information see: <https://trac.videolan.org/vlc/ticket/11162>

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

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

Web www.security-assessment.com

Email info@security-assessment.com