Vulnerability Advisory

Name	AVID Media Composer Phonetic Indexer Remote Stack Buffer Overflow
Vendor Website	http://www.avid.com
Date Released	November 29, 2011
Affected Software	AVID Media Composer <= 5.5.3
Researcher	Nick Freeman (nick.freeman@security-assessment.com)

Description

Security-Assessment.com discovered a remote stack buffer overflow vulnerability in a network daemon that ships with Avid Media Composer 5.5, named AvidPhoneticIndexer.exe. By sending a large request to the listening network service, it is possible to overwrite the stack of the process and gain arbitrary code execution.

Exploitation

An exploit for this vulnerability can be found on the Security-Assessment.com website at http://security-assessment.com/files/avid_phonetic_indexer.rb. This will be present in the Metasploit framework in the near future.

Solution

No patch is available for this vulnerability at this time. Host and network based firewalling are recommended as workarounds to limit the exposure of the vulnerable service.

Disclosure timeline

Security-Assessment.com practices responsible disclosure and made significant effort to report this vulnerability to AVID.

14/05/11: Vulnerability identified.
17/05/11: Avid Media Composer 5.5.2 released.
26/05/11: Attempted calling, left voicemail and emailed the AVID Application Security Management team.
Early June 2011: Called members of the AVID Media Composer Development team.
Early-Mid June 2011: Emailed AVID Media Composer Product Management team, who indicated that they were aware of the vulnerabilities before I had explained the nature of the issues. AVID explained that all vulnerabilities were in the process of being resolved. Security-Assessment.com suggested collaboration to ensure all issues were being identified, but AVID was not interested in pursuing this.
17/08/11: Avid Media Composer 5.5.3 released. Vulnerability still present.
05/11/11: Vulnerability released at Kiwicon V in Wellington, New Zealand.
19/11/11: Vulnerability released at Ruxcon 2011 in Melbourne, Australia.
29/11/11: Vulnerability advisory and exploit code published.

About Security-Assessment.com

Security-Assessment.com is Australasia's 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.