

microsoft.public.security.virus: February 05, CNET News – RealPlayer flaws open PCs up to hijackers.

February 05, CNET News – RealPlayer flaws open PCs up to hijackers.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-02/0782.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 02/09/04

Date: Mon, 9 Feb 2004 10:35:28 -0500

February 05, CNET News – RealPlayer flaws open PCs up to hijackers. RealNetworks acknowledged on Wednesday that three flaws affecting different versions of its media player could allow attackers to create corrupt music or video files that, when played, take control of a victim's PC. The flaws can affect RealNetworks' RealOne Player, RealOne Player version 2, RealPlayer 8, RealPlayer 10 Beta, and the company's RealOne Enterprise products. To exploit them, an attacker crafts the data in a media file in a certain way. When people play or stream the corrupted file in a vulnerable version of RealPlayer, the attacker's code will run, compromising the PC. The vulnerabilities may affect a large portion of the 350 million unique registered users of the media player software, but RealNetworks wouldn't say how many of those people use the vulnerable versions. The flaw can be exploited using a specially crafted media file, which can be one of five types: RealAudio (RAM) file, RealAudio Plugin (RPM) file, RealPix (RP) file, RealText (RT) file or synchronized multimedia integration language (SMIL) file.

Source: http://news.com.com/2100-7349_3-5154193.html?tag=nefd_top

-----Original Message-----

From: CIAC Mail User [mailto:ciac@rum.llnl.gov]

Sent: Friday, February 06, 2004 5:25 PM

To: bulletin-list@rum.llnl.gov

Subject: CIAC BULLETIN O-075 RealPlayer / RealOne Player Buffer Overrun Vulnerabilities

[For Public Release]

-----BEGIN PGP SIGNED MESSAGE-----

The U.S. Department of Energy
Computer Incident Advisory Capability

/|/_\|/
_ _|_ / \ _

INFORMATION BULLETIN

microsoft.public.security.virus: February 05, CNET News – RealPlayer flaws open PCs up to hijackers.

RealPlayer / RealOne Player Buffer Overrun Vulnerabilities
[RealNetworks, 02/06/04]

February 6, 2004 21:00 GMT Number O-075

PROBLEM: Buffer overrun vulnerabilities have been identified on Real Players and RealOne Players. These are popular programs installed on most operating systems for streaming video and audio feeds over the Internet.

PLATFORM: RealOne Player and RealPlayer 8 (all language versions)
RealOne Player v2 for Windows only (all languages)
RealOne Enterprise Desktop or RealPlayer Enterprise (all versions)
RealPlayer 10 Beta (English only)

DAMAGE: By crafting malformed .RP, .RT, .RAM, .RPM & .SMIL files it is possible to cause a system to download and run arbitrary code or cause a buffer overrun error.

SOLUTION: Install the vendor's updates.

VULNERABILITY The risk is **MEDIUM**. A remote attacker could execute arbitrary **ASSESSMENT:** code running in the context of the logged on user.

LINKS:

CIAC BULLETIN: <http://www.ciac.org/ciac/bulletins/o-075.shtml>

ORIGINAL BULLETIN: http://service.real.com/help/faq/security/040123_player/EN/

-----BEGIN PGP SIGNATURE-----

Version: 4.0 Business Edition

iQCVAwUBQCQUH7nzJzdsy3QZAQEKgQP+IINcAVEFmO5JRLSUGkhBT3ihh4ZMbcGm
C99d8+zYUfNVdQ+5kI/+vC25ZWAw+bcpKLJbMB2FWVMMUYOtt4ThFQHpNMGCCfM/
BxJHik/43sUIFgMRf3V4jxnDKtXv+UrkYAGYReLBpLsmFHAsR3/cNxwEoPNUGNB
RnDPXFXHFQU=
=MDC3

-----END PGP SIGNATURE-----

CIAC LIST: 12