US-CERT - Later than CyTRAP Labs RealPlayer

2007-10-24 21:19 hours GMT

2007-10-19 – late afternoon Friday Pacific Standard Time RealNetworks released patch

This was a zero-day exploit (we released an zero-day alert on 2007-11-18) whereby hackers were actively exploiting this vulnerability – **US-CERT did not inform about** zero-day exploit (http://info.cytrap.eu/?page_id=111) and how to minimize one's risk exposure. Patch was available 2007-11-20 – CyTRAP Labs informed subscribers that same day = 5.2 days before US-CERT

http://casescontact.org/alerts/110116 (see our advisory)

Date: Wed, 24 Oct 2007 15:24:46 -0400
From: US-CERT Alerts <alerts@us-cert.gov>
To: alerts@us-cert.gov
Organization: US-CERT - +1 202-205-5266
List-Id: US-CERT Alerts <alerts.us-cert.gov>
List-Help: <http://www.us-cert.gov/cas/#non-tech>, <mailto:Majordomo@us-cert.gov?body=help>
List-Subscribe: <mailto:Majordomo@us-cert.gov?body=subscribe%20alerts>
List-Unsubscribe: <mailto:Majordomo@us-cert.gov?body=unsubscribe%20alerts>
List-Post: NO (posting not allowed on this list)
List-Archive: <http://www.us-cert.gov/cas/alerts>
Subject: US-CERT Cyber Security Alert SA07-297A -- RealNetworks RealPlayer ActiveX Playlist Vulnerability

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

National Cyber Alert System
Cyber Security Alert SA07-297A

RealNetworks RealPlayer ActiveX Playlist Vulnerability

Original release date: October 24, 2007
Last revised: --
Source: US-CERT

Systems Affected

* RealPlayer 11 beta
* RealPlayer 10.5
* RealPlayer 10
* RealOne Player v2
* RealOne Player

Overview

RealNetworks RealPlayer for Microsoft Windows contains a vulnerability that could allow an attacker to take control of your computer when you visit a malicious web site.

Solution

Upgrade and install a patch

RealNetworks has released a patch to address this vulnerability. Information about the vulnerability and the patch is available in RealPlayer Security Vulnerability and Security Update for Real Player.

* RealPlayer 10.5 and RealPlayer 11 beta users should install the patch.
* RealOne Player v2, and RealPlayer 10 users should upgrade to RealPlayer 10.5 or RealPlayer 11 beta and then install the patch.

Windows versions of RealPlayer 8 and earlier are not affected. Mactintosh and Linux versions of RealPlayer are not affected.

Disable ActiveX for untrusted web sites

Disabling ActiveX in the Internet Zone (or any zone used by an attacker) reduces the chances of exploitation of this and other vulnerabilities. Instructions for disabling ActiveX in the Internet Zone can be found in the "Securing Your Web Browser" document.

There are public reports that this vulnerability is being actively exploited.

Description

A buffer overflow in the way RealPlayer handles playlists received from an ActiveX control on a web page could allow an attacker to access your computer, install and run malicious software on your computer, or cause it to crash.

More technical information is available in US-CERT Technical Cyber Security Alert TA07-297A and Vulnerability Note VU#871673.

References

* RealNetworks RealPlayer Security Update - <http://service.real.com/realplayer/security/191007_player/en/>

* Security Update for RealPlayer - <http://docs.real.com/docs/security/SecurityUpdate101907Player.pdf>

* US-CERT Technical Cyber Security Alert TA07-297A -
  <http://www.us-cert.gov/cas/techalerts/TA07-297A.html>

* US-CERT Vulnerability Note VU#871673 -
  <http://www.kb.cert.org/vuls/id/871673>

* Securing Your Web Browser -
  <http://www.us-cert.gov/reading_room/securing_browser/#Internet_Explorer>

The most recent version of this document can be found at:

  <http://www.us-cert.gov/cas/alerts/SA07-297A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "SA07-297A Feedback VU#871673" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Revision History

  October 24, 2007: Initial release

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRx+bRPRFkHkM87XOAQK5tQf/ZMQAEfnLtS3QTAtayioNbJ4hB3ccG73H
ew/1cw7H4jxOuNVyIeHcExKfddkR0+MXWnhreTfx1obN7dBc7CfaNqfsO9eJow1h
57Isp8dRzWnysdrLggZLq8EBqVo0X+Cw8AU7Db9CC/ciL43B45hkCXmfQrjK7pgB
L3V2CLROQapEXq08N0WG1h6ViW9eLqCEcnYPR+X3L+roI6C0/B6pHqf/xlVznKPL
67VM8v40kVEf2ARh/jfDe2TCqOWBqB/nqUz5RT8/bl7vqjqdZm/QwecxPqPTZIPM
YwJVB578Eqz+KqZISS7te3vSRp51Abg8mtSgBsSrSjiYSUISteEoAA==
=W+3F
-----END PGP SIGNATURE-----

Adobe update

US-CERT - Later than CyTRAP Labs Adobe Reader

2007-10-24 21:19 hours GMT

2007-10-23 –Pacific Standard Time Adobe released patch

This was a zero-day exploit (we announced 2007-09-21) whereby hackers were actively exploiting this vulnerability – **service did not inform about** zero-day exploit (http://info.cytrap.eu/?page_id=111) and how to minimize one's risk exposure. Patch was available 2007-11-23 – CyTRAP Labs informed - 1.75 days faster http://casescontact.org/alerts/110114

2007-10-25 – CyTRAP informed users about Foxit software having decided to not release a patch for Foxit Reader (free reader – has same vulnerability like Adobe Reader) until next scheduled patch release

Date: Wed, 24 Oct 2007 18:19:55 -0400
From: US-CERT Alerts <alerts@us-cert.gov>
To: alerts@us-cert.gov
Organization: US-CERT - +1 202-205-5266
List-Id: US-CERT Alerts <alerts.us-cert.gov>
List-Help: <http://www.us-cert.gov/cas/#non-tech>, <mailto:Majordomo@us-cert.gov?body=help>
List-Subscribe: <mailto:Majordomo@us-cert.gov?body=subscribe%20alerts>
List-Unsubscribe: <mailto:Majordomo@us-cert.gov?body=unsubscribe%20alerts>
List-Post: NO (posting not allowed on this list)
List-Archive: <http://www.us-cert.gov/cas/alerts>
Subject: US-CERT Cyber Security Alert SA07-297B -- Adobe Updates for Microsoft Windows Vulnerability

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

National Cyber Alert System
Cyber Security Alert SA07-297B

Adobe Updates for Microsoft Windows Vulnerability

Original release date: October 24, 2007
Last revised: --
Source: US-CERT

Systems Affected

Microsoft Windows XP and Windows Server 2003 systems with Internet Explorer 7 and any of the following Adobe products:

* Adobe Reader 8.1 and earlier
* Adobe Acrobat Professional, 3D, and Standard 8.1 and earlier
* Adobe Reader 7.0.9 and earlier
* Adobe Acrobat Professional, 3D, Standard, and Elements 7.0.9 and earlier

Overview

Microsoft Windows XP and Server 2003 systems with Internet Explorer 7 contain a vulnerability that could allow an attacker to take control of your computer by convincing you to open a malicious PDF document. Public reports indicate that this vulnerability is being actively exploited.

Solution

Apply an update

Adobe has released Adobe Reader 8.1.1 and Adobe Acrobat 8.1.1 to address this issue. Please see Adobe Security Bulletin APSB07-18 for details.

Description

Microsoft Windows XP and Server 2003 systems with Internet Explorer 7 installed contain a vulnerability in the way Windows determines the appropriate program to handle data specified in a Uniform Resource Identifier (URI). An attacker can exploit this vulnerability by convincing you to open a specially crafted PDF document. The attacker could gain access your computer, install and run malicious software on your computer, or cause it to crash.

More technical information is available in US-CERT Technical Cyber Security Alert TA07-297A and Vulnerability Note VU#403150.

References

* Adobe Security Bulletin APSB07-18 - <http://www.adobe.com/support/security/bulletins/apsb07-18.htm>

* Microsoft Security Advisory (943521) - <http://www.microsoft.com/technet/security/advisory/943521.mspx>

* US-CERT Vulnerability Note VU#403150 - <http://www.kb.cert.org/vuls/id/403150>

* US-CERT Technical Alert TA07-297B - <http://www.us-cert.gov/cas/techalerts/TA07-297B.html>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/alerts/SA07-297B.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "SA07-297B Feedback VU#403150" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Revision History

October 24, 2007: Initial release

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iQEVAwUBRx/EX/RFkHkM87XOAQKFVgf/WqSe7r3gseKvxUCUFTvJhMxr+QAB23mp
Bhz7/J65ZMUxKr5YBjMM1vELRZs0rCJyjY6Y4f4+Ig9d5tI7JQnGI6b/5zmJRAst
A4waHADS//AnwXwnZOTvs/eKDfyfKrMakwmUWAaSxqkk6O6yqKdp4toSq2KK3qMz
PsN4FFxNWZFMijONzpeoRo34aSg+ZUwAMbHDhs2A9My0g0I9aCfkQQT9X0S7qDIA
V3t4sCTNK3/uWIBO5P/YEM6TJeWLgcYxsCtbUxaETKxRme3m72gQPEQL6EwPG+nv
y10fLt104XewAPl5V32GWdvop9czbQI9mJeCYaeZPTBLi1RITYWFtQ==
=Mjf+
-----END PGP SIGNATURE-----