

[Full-disclosure]

<http://www.zerodayinitiative.com/advisories/ZDI-08-046>

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-07/msg00471.html>

- *From:* zdi-disclosures@xxxxxxxx
 - *Date:* Fri, 25 Jul 2008 16:27:06 -0500
-

ZDI-08-046: RealNetworks RealPlayer Library File Deletion Stack Overflow Vulnerability
<http://www.zerodayinitiative.com/advisories/ZDI-08-046>
July 25, 2008

-- CVE ID:
ZDI-CAN-231

-- Affected Vendors:
RealNetworks

-- Affected Products:
RealNetworks RealPlayer

-- TippingPoint(TM) IPS Customer Protection:
TippingPoint IPS customers have been protected against this vulnerability by Digital Vaccine protection filter ID 5734.
For further product information on the TippingPoint IPS, visit:

<http://www.tippingpoint.com>

-- Vulnerability Details:
This vulnerability allows remote attackers to execute arbitrary code on systems with vulnerable installations of the RealNetworks RealPlayer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists in RealPlayer's rjbdll.dll module when handling the deletion of media library files. An attacker could exploit this vulnerability using an ActiveX control {FDC7A535-4070-4B92-A0EA-D9994BCC0DC5} to import a vulnerable file into the user's media library. Upon deletion of this file, an exploitable stack based buffer overflow can be triggered.

-- Vendor Response:
RealNetworks has issued an update to correct this vulnerability. More details can be found at:

http://service.real.com/realplayer/security/07252008_player/en/

— Disclosure Timeline:

2007-11-02 – Vulnerability reported to vendor

2008-07-25 – Coordinated public release of advisory

— Credit:

This vulnerability was discovered by:

* Anonymous

— About the Zero Day Initiative (ZDI):

Established by TippingPoint, The Zero Day Initiative (ZDI) represents a best-of-breed model for rewarding security researchers for responsibly disclosing discovered vulnerabilities.

Researchers interested in getting paid for their security research through the ZDI can find more information and sign-up at:

<http://www.zerodayinitiative.com>

The ZDI is unique in how the acquired vulnerability information is used. TippingPoint does not re-sell the vulnerability details or any exploit code. Instead, upon notifying the affected product vendor, TippingPoint provides its customers with zero day protection through its intrusion prevention technology. Explicit details regarding the specifics of the vulnerability are not exposed to any parties until an official vendor patch is publicly available. Furthermore, with the altruistic aim of helping to secure a broader user base, TippingPoint provides this vulnerability information confidentially to security vendors (including competitors) who have a vulnerability protection or mitigation product.

Our vulnerability disclosure policy is available online at:

http://www.zerodayinitiative.com/advisories/disclosure_policy/

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is being sent by 3Com for the sole use of the intended recipient(s) and may contain confidential, proprietary and/or privileged information. Any unauthorized review, use, disclosure and/or distribution by any recipient is prohibited. If you are not the intended recipient, please delete and/or destroy all copies of this message regardless of form and any included attachments and notify 3Com immediately by contacting the sender via reply e-mail or forwarding to 3Com at postmaster@xxxxxxxx

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>