

[REVS] Analysis of Real Network's RealServer Remote Root Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0004.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/01/04

To: list@securiteam.com

Date: 1 Oct 2004 11:07:04 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Analysis of Real Network's RealServer Remote Root Exploit

SUMMARY

Linked below is a detailed analysis of the vulnerability found in RealServer. Michael H. Lastor's paper focuses on <http://www.securiteam.com/exploits/5JP0B1F96W.html> THC's exploit and provides a detailed analysis. Additionally a real life intrusion example with this exploit is given and what to do, after you got root is exemplified.

DETAILS

Abstract:

In this paper, we will examine the root vulnerability in RealNetworks servers, which include: Helix Universal Server 9, RealSystem Server version 8, version 7 and RealServer G2. When this exploit is used against one of the vulnerable versions of RealNetworks Servers, it will provide a root shell listening on port 31337. Dave Aitel of Immunitysec is the one who found the bug and posted the vulnerability into various bulletin boards. Johnny Cyberpunk of THC (The Hackers Choice) is the one who has released the exploit code to the public. Through the use of the exploit code in a lab environment, this paper will show how the exploit code can be used to perform final reconnaissance of the target system and to launch

Securiteam: [REVS] Analysis of Real Network's RealServer Remote Root Exploit

the attack code. A review of the exploit code along with captured packets will explain, in detail, what the exploit code is doing. Next, is a fictitious scenario showing the five phases that an attacker will go through while using this exploit. Lastly, we will continue the fictitious scenario from the perspective of the incident handler. This will take the reader through the six steps that an Incident Handler goes through while handling an incident.

ADDITIONAL INFORMATION

The whitepaper can be found at:

<http://www.thc.org/root/docs/exploit_analysis/REALSERVER_EXPLOIT_ANALYSIS.PDF>
http://www.thc.org/root/docs/exploit_analysis/REALSERVER_EXPLOIT_ANALYSIS.PDF

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.