Updated April 2, 2012

RealNetworks is making available product upgrades that contain security bug fixes.

RealNetworks, Inc. has addressed two recently discovered security vulnerabilities. RealNetworks takes all security vulnerabilities extremely seriously and provides this information as an aid for users to avoid potential exploits.

VULNERABILITY DESCRIPTIONS:

CVE-2012-1923 Secunia Advisory SA45414 –
Secunia Research has discovered multiple vulnerabilities in RealNetworks Helix Server, which can be exploited by malicious, local users to disclose sensitive information and by malicious people to cause a DoS (Denial of Service).

Part 1 clear text passwords
The administrative and user credentials are insecurely stored in the flat file database (\Program Files\Real\Helix Server\adm_b_db\users\), which can be exploited by local users to disclose the clear text passwords.

> Fix: For users concerned about the Helix Server machine's file system being vulnerable, the workaround is to initially change the permissions of the folder that contains authentication databases to be restricted to only administrators. This will encrypt the password for all newly stored passwords. Existing accounts must be updated with a new password to encrypt the password using Digest.

Part 2 telnet to 705 crashes SNMP Master Agent
An error in the SNMP Master Agent process (master.exe) can be exploited to terminate the service by establishing and immediately closing a TCP connection on port 705.

Part 3 validation error on "DisplayString" crashes SNMP Master Agent
An input validation error when processing the "DisplayString" of SNMP object identifiers can be exploited to cause an unhandled exception and terminate the SNMP Master Agent service (master.exe) via a specially crafted "Open-PDU" request sent to TCP port 705.

CVE-2012-0942:
RealNetworks Helix Server rn5auth Credential Parsing Remote Code Execution Vulnerability

A bug exists in the code which parses authentication credentials and allows for a buffer overflow.

CVE-2012-1984 MSVR-11-124: Multiple XSS Vulnerabilities
Real Networks Helix Server version 14.2.0.212 is vulnerable to multiple cross site scripting vulnerabilities.

CVE-2012-1985 MSVR-11-125: Malformed URL Stack Exhaustion
Real Networks Helix Universal Media Server version 14.2.0.212 contains a flaw where a malformed URL can cause the server process to crash. We consider this vulnerability to be of low severity due to the fact that an attacker would have to leverage a cross-site request forgery (csrf) attack in order to trick the administrator in to load the malformed URL.

SOLUTION:
The vulnerabilities are resolved on the following platforms by installing Version 14.3.x of the Helix Server and the Helix Mobile Server. This only pertains to supported versions of the platforms listed below.
--- Red Hat Enterprise Linux 5
--- Sun Solaris 10
--- Windows 2008

Impacted Products and Versions:
--- Helix Server Version 14.x
--- Helix Mobile Server Version 14.x

ACKNOWLEDGMENT:
RealNetworks would like to thank Dmitriy Pletnev of Secunia Research,
Derek Brown of TippingPoint's Zero Day Initiative, and Tom Gallagher at Microsoft and Microsoft Vulnerability Research (MSVR) for bringing these exploits to our attention.

WARRANTY: