CERT Advisory CA-2002-35 Vulnerability in RaQ Server Appliances

Original release date: December 11, 2002
Last revised: Tue Dec 17 14:43:22 EST 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Cobalt RaQ 4 Server Appliances with the Security Hardening Package installed
- Sun Cobalt RaQ 3 Server Appliances running the RaQ 4 build with the Security Hardening Package installed

Overview

A remotely exploitable vulnerability has been discovered in Sun Cobalt RaQ Server Appliances running Sun's Security Hardening Package (SHP). Exploitation of this vulnerability may allow remote attackers to execute arbitrary code with superuser privileges.

I. Description

Cobalt RaQ is a Sun Server Appliance. Sun provides a Security Hardening Package (SHP) for Cobalt RaQs. Although the SHP is not installed by default, many users choose to install it on their RaQ servers. For background information on the SHP, please see the SHP RaQ 4 User Guide.

A vulnerability in the SHP may allow a remote attacker to execute arbitrary code on a Cobalt RaQ Server Appliance. The vulnerability occurs in a cgi script that does not properly filter input. Specifically, *overflow.cgi* does not adequately filter input destined for the *email* variable. Because of this flaw, an attacker can use a POST request to fill the *email* variable with arbitrary commands. The attacker can then call *overflow.cgi*, which will allow the command the attacker filled the *email* variable with to be executed with superuser privileges.

An exploit is publicly available and may be circulating.

Further information about this vulnerability may be found in VU#810921 in the CERT/CC Vulnerability Notes Database.

II. Impact

A remote attacker may be able to execute arbitrary code on a Cobalt RaQ Server Appliance with the SHP installed.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Workarounds

Block access to the Cobalt RaQ administrative httpd server (typically ports 81/TCP and 444/TCP) at your network perimeter. Note that this will not protect vulnerable hosts within your network perimeter. It is important to understand your network configuration and service requirements before deciding what changes are appropriate.

Caveats

The patch supplied by Sun removes the SHP completely. If your operation requires the use of the SHP, you may need to find a suitable alternative.

Appendix A. - Vendor Information

Sun Microsystems

Sun confirms that a remote root exploit does affect the Sun/Cobalt RaQ4 platform if the SHP (Security Hardening Patch) patch was installed.

Sun has released a Sun Alert which describes how to remove the SHP patch:

http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/49377

The removal patch is available from:

http://ftp.cobalt.sun.com/pub/packages/raq4/eng/RaQ4-en-Security-2.0.1-SHP_REM.pkg

Appendix B. - References

1. CERT/CC Vulnerability Note: VU#810921 - http://www.kb.cert.org/vuls/id/810921
2. Sun SHP RaQ 4 User Guide - http://www.sun.com/hardware/serverappliances/pdfs/support/RaQ_4_SHP_UG.pdf
3. COBALT RaQ 4 User Manual - http://www.sun.com/hardware/serverappliances/pdfs/manuals/manual.raq4.pdf

---

grazer@digit-labs.org publicly reported this vulnerability.

Author: Ian A. Finlay.

Copyright 2002 Carnegie Mellon University.

Revision History

```
December 11, 2002: Initial release
December 16, 2002: Added information stating RaQ 3 Server Appliances are vulnerable as well (with SHP installed)
December 16, 2002: Revised systems affected section
```