Immunity, Inc. Advisory

Disclosure

This advisory is has been released to the public, and may be retransmitted without modification.

Vulnerability

Remote, unauthenticated certificate upload in Compaq Web Management (HP HTTP)

Compaq Web Management includes a number of daemons, which listen on a number of TCP ports, and also to SNMP requests. On port 2381, an SSL HTTP server runs. If the system is configured to let anonymous users browse it, a common configuration, then a bug in the validation system allows users to upload their own certificates to be trusted by the client system. This would then allow that machine to be administered remotely via such mechanisms as Secure Task Execution.

This is considered a critical problem, as Compaq Web Management is often installed on every machine in an enterprise.

This bug is exploitable, and can be done over and over. No knowledge of the Windows version is needed to be effective. This would probably work on all the other systems supported by Compaq Web Management.

Insight Manager 7 can be used to create valid certificates for this attack.

Other Notes

Patch URL:

http://h18023.www1.hp.com/support/files/Server/us/download/20197.html

Patch Date: March 11, 2004

HP Case ID: SSRT4679 HP Web-enabled Management Software certificate compromise using HP HTTP Server

Patched Version: HP HTTP 5.93

Vulnerable Versions: Version 5.0 through Version 5.92

Default Configuration: Not vulnerable, since anonymous access is turned off by default. In Immunity's experience, anonymous access is often turned on due to company policies that require it for interoperability or other reasons.

Affected

All known versions of Compaq Web Management are affected. Version 5 and 7 were tested. All products which include vulnerable versions of HP HTTP should be considered affected.

Detection

Immunity Research has provided working exploits for these problems. (See your CANVAS distribution)

For questions or comments, please contact Immunity, Inc. at dave@immunitysec.com, or http://www.immunitysec.com.

History

Found by Immunity Researcher Dave Aitel, October, 2003.