security-assessment.com

Vulnerability Advisory

Name	Aerohive Hive Manger and Hive OS Multiple Vulnerabilities
Vendor Website	http://www.aerohive.com
Affected Software	Aerohive Hive Manager (Stand-alone and Cloud) <= 6.1R3 and HiveOS 6.1R3
Date Released	28/08/2014
Author	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Aerohive Hive Manager and HiveOS software. These vulnerabilities have been disclosed to the vendor on or before the 24th of April 2014.

Hive Manager Arbitrary File Disclosure

Leveraging directory traversal, a malicious user can retrieve arbitrary files from the Hive Manager file system. As the Tomcat instance serving the Hive Manager software runs as the root user, this vulnerability can be used to read any file off the file system, including sensitive files such as /etc/shadow.

Hive Manager Arbitrary File Upload

An authenticated malicious user may send a crafted post to the 'upload' servlet and upload arbitrary files. As the upload servlet is protected by HTTP basic authentication, this requires the knowledge of the scpuser's password.

Hive Manager Debugserver Code Execution

It was discovered that an authenticated user may send a crafted request to the Hive Manager 'debugserver' servlet and execute arbitrary commands on the Hive Manager server.

Hive Manager Multiple Password Disclosure

Multiple methods within the Hive Manager web interface were found to expose sensitive information such as usernames and passwords. A malicious entity may leverage these disclosures to further compromise the Hive Manager.

Hive Manager Reflected Cross Site Scripting

Multiple Reflected Cross Site Scripting vulnerabilities were found within the Hive Manager software. These vulnerabilities allow a malicious entity to potentially gain JavaScript execution within a legitimate user's browser. This is done with the aim of harming the user's browser or hijacking their session.

Hive Manager SSH Keys Lacking Passphrase

An SSH key was found on the Hive Manager file system without any passphrase set. This allows a malicious user with access to the file system to gain unauthorised access to the system with root user privileges.

Hive Manager Subshell Bypass

By using a crafted SSH command, a malicious user may gain root access to the Hive Manager with a fully functional bash terminal, effectively bypassing the Aerohive subshell. This allows the malicious user to perform tasks on the underlying CentOS Linux operating system, including the retrieval of private keys, passwords and other sensitive information

Hive Manager Unauthenticated Arbitrary File Upload

The Hive Manager HHMUploadServlet was found to suffer from an Unauthenticated Arbitrary File Upload vulnerability. By sending a crafted packet to the servlet, a malicious entity is able to gain arbitrary code execution on the Hive Manager server.

Copyright Security-Assessment.com 2014

HiveOS Local File Inclusion

Aerohive HiveOS was found to contain a Local File Inclusion Vulnerability within the web administrative interface.

The Local File Inclusion allows a malicious entity to control what files are included by the vulnerable PHP page. In the event that the malicious entity is able to control an element on the file system, this results in arbitrary code execution. As user controlled information is present within the log-files of the application, this is easily achievable.

HiveOS Password Disclosure

Log files within the HiveOS operating system were found to disclose sensitive information such as usernames and password. A malicious user may leverage this information to further compromise the Aerohive deployment or its users.

HiveOS Unauthenticated Firmware Upload

Insufficient authorisation checking was found to be being performed on certain firmware upload functions. This allows for the upload of a backdoored or otherwise malicious firmware by an attacker.

Exploitation

Detailed exploitation information and code will be released in December 2014.

Solution

Update to the latest version of Hive Manager and HiveOS software including the cloud solutions.

Responsible Disclosure Policy

Security-Assessment.com follows a responsible disclosure policy where we typically offer 90 days before publicly disclosing a vulnerability and a further 90 days before releasing exploit code or detailed examples for the vulnerability.

Researchers

Denis Andzakovic, Scott Bell, Nick Freeman, Thomas Hibbert, Carl Purvis, Pedro Worcel.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650

Copyright Security-Assessment.com 2014