Scan Report

October 13, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone UTC , which is abbreviated UTC . The task was pruebas123 . The scan started at Tue Oct 13 05:19:50 2020 UTC and ended at Tue Oct 13 05:37:43 2020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.2.104	2	2	0	0	0
Total: 1	2	2	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level Log are not shown.
Issues with the threat level Debug are not shown.
Issues with the threat level False Positive are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 4 results selected by the filtering described above. Before filtering there were 26 results.

2 Results per Host

2.1 192.168.2.104

Host scan start Tue Oct 13 05:20:53 2020 UTC
Host scan end Tue Oct 13 05:37:04 2020 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
135/tcp	Medium

2.1.1 High 80/tcp

High (CVSS: 7.5)
NVT: HTTP File Server Remote Command Execution Vulnerability-01 Jan16

Product detection result
cpe:/a:httpfilesever:hfs:2.3
Detected by Http File Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.806812 ,→)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running HTTP File Server and is prone to remote command execution vulnerability.

Vulnerability Detection Result
Installed Version: 2.3
Fixed Version: 2.3d

Impact

Successful exploitation will allow an attacker to execute arbitrary code by uploading a file with certain invalid UTF-8 byte sequences that are interpreted as executable macro symbols.

Solution
Solution type: VendorFix
Update to version 2.3d or later.

Affected Software/OS
HttpFileServer version 2.3c and prior.

Vulnerability Insight
The flaw is due to the application does not properly validate uft-8 broken byte representation

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: HTTP File Server Remote Command Execution Vulnerability-01 Jan16
OID:1.3.6.1.4.1.25623.1.0.806813

Product Detection Result
Product: cpe:/a:httpfilesever:hfs:2.3
Method: Http File Server Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.806812)

References
cve: CVE-2014-7226
bid: 70216
url: https://packetstormsecurity.com/files/128532
url: http://www.rejetto.com/hfs

High (CVSS: 7.5)
NVT: HTTP File Server Remote Command Execution Vulnerability-02 Jan16

Product detection result
cpe:/a:httpfilesever:hfs:2.3
Detected by Http File Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.806812 ,→)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is running HTTP File Server and is prone to remote command execution vulnerability.

Vulnerability Detection Result
Installed Version: 2.3
Fixed Version: Not available

Impact
Successful exploitation will allow an attacker to execute arbitrary code by uploading a file with certain invalid UTF-8 byte sequences that are interpreted as executable macro symbols.

Solution
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnera bility. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
HttpFileServer version 2.3g and prior.

Vulnerability Insight
The flaw is due to an improper neutralization of Null byte or NUL character

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: HTTP File Server Remote Command Execution Vulnerability-02 Jan16
OID:1.3.6.1.4.1.25623.1.0.806814

Product Detection Result
Product: cpe:/a:httpfilesever:hfs:2.3
Method: Http File Server Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.806812)

References
cve: CVE-2014-6287
bid: 69782
url: http://packetstormsecurity.com/files/128593
url: https://www.kb.cert.org/vuls/id/251276
url: https://www.exploit-db.com/exploits/39161/

[return to 192.168.2.104]

2.1.2 Medium 80/tcp

2 RESULTS PER HOST 5

Medium (CVSS: 5.0)
NVT: Missing `httpOnly` Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
The cookies:
Set-Cookie: HFS_SID=0.246919495984912; path=/;
are missing the "httpOnly" attribute.

Solution
Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: Missing `httpOnly` Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.105925

References
url: https://www.owasp.org/index.php/HttpOnly
url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-00 ,→2)

[return to 192.168.2.104]

2.1.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p ,→rotocol:

. . . continues on next page . . .

. . . continued from previous page . . .

```
Port: 49664/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.104[49664]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.104[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.104[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.2.104[49664]
      Annotation: KeyIso
Port: 49665/tcp
```

```
          UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49665]
   Port: 49666/tcp
          UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49666]
          UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49666]
   Port: 49667/tcp
          UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49667]
          Annotation: Event log TCPIP
   Port: 49668/tcp
          UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49668]
          UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49668]
          Named pipe : spoolss
          Win32 service or process : spoolsv.exe
          Description : Spooler service
          UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49668]
          UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49668]
          UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49668]
   Port: 49669/tcp
          UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
          Endpoint: ncacn_ip_tcp:192.168.2.104[49669]
   Port: 49745/tcp
          UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
          Endpoint: ncacn_ip_tcp:192.168.2.104[49745]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
          Annotation: Remote Fw APIs
   Note: DCE/RPC or MSRPC services running on this host locally were identified. Re ,→porting
   this list is not enabled by default due to the possible large size of ,→this list. See the script
   preferences to enable this reporting.
```

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution

Solution type: Mitigation

Filter incoming traffic to this ports.

Vulnerability Detection Method

Details: DCE/RPC and MSRPC Services Enumeration Reporting

OID:1.3.6.1.4.1.25623.1.0.10736

[return to 192.168.2.104]