Vulnerabilities by Host

- 192.168.100.5
Vulnerabilities by Host
Scan Information

Start time: Mon Mar 30 03:55:39 2020
End time: Mon Mar 30 03:56:23 2020

Host Information

IP: 192.168.100.5
OS: Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8

Vulnerabilities

77829 - GNU Bash Environment Variable Handling Code Injection (Shellshock)

Synopsis

The remote web server is affected by a remote code execution vulnerability.

Description

The remote web server is affected by a command injection vulnerability in GNU Bash known as Shellshock. The vulnerability is due to the processing of trailing strings after function definitions in the values of environment variables. This allows a remote attacker to execute arbitrary code via environment variable manipulation depending on the configuration of the system.

See Also

http://seclists.org/oss-sec/2014/q3/650
http://www.nessus.org/u?dacf7829
https://www.invisiblethreat.ca/post/shellshock/

Solution

Apply the referenced patch.

Risk Factor

Critical
CVSS v3.0 Base Score


CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BID</td>
<td>70103</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE-2014-6271</td>
</tr>
<tr>
<td>XREF</td>
<td>CERT:252743</td>
</tr>
<tr>
<td>XREF</td>
<td>EDB-ID:34765</td>
</tr>
<tr>
<td>XREF</td>
<td>EDB-ID:34766</td>
</tr>
<tr>
<td>XREF</td>
<td>EDB-ID:34777</td>
</tr>
</tbody>
</table>

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/09/24, Modified: 2019/11/25

Plugin Output

tcp/80

Nessus was able to exploit the issue using the following request:

GET /cgi-bin/vuln.cgi HTTP/1.1
Host: 192.168.100.5
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo ; echo ; /usr/bin/id;
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/png, */*

This produced the following truncated output (limited to 2 lines) :
--------------------------------- snip ---------------------------------
uid=1000(hca) gid=50(staff) groups=50(staff)
--------------------------------- snip ---------------------------------
82581 - GNU Bash Incomplete Fix Remote Code Injection (Shellshock)

Synopsis

The remote web server is affected by a remote code execution vulnerability.

Description

The remote web server is affected by a command injection vulnerability in GNU Bash known as Shellshock. The vulnerability is due to the processing of trailing strings after function definitions in the values of environment variables. This allows a remote attacker to execute arbitrary code via environment variable manipulation depending on the configuration of the system.

Note that this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

See Also

http://lcamtuf.blogspot.com/2014/10/bash-bug-how-we-finally-cracked.html
http://www.nessus.org/u?dacf7829

Solution

Apply the referenced patch.

Risk Factor

Critical

CVSS v3.0 Base Score


CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I
References

BID  70166
CVE  CVE-2014-6278

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2015/04/06, Modified: 2019/11/22

Plugin Output

tcp/80

Nessus was able to exploit the issue using the following request:

GET /cgi-bin/vuln.cgi HTTP/1.1
Host: 192.168.100.5
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: () { _; } >$_{${$()}} { echo Content-Type: text/plain ; echo ; echo ; /usr/bin/id; }
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

This produced the following truncated output (limited to 2 lines):

uid=1000(hca) gid=50(staff) groups=50(staff)
11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis
Debugging functions are enabled on the remote web server.

Description
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

Solution
Disable these methods. Refer to the plugin output for more information.

Risk Factor
Medium

CVSS v3.0 Base Score
5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score
4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score
3.7 (CVSS2#E:U/RL:OF/RC:C)

References
BID 9506
BID 9561
BID 11604
BID 33374
To disable these methods, add the following lines for each virtual host in your configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request:

```
TRACE /Nessus661699624.html HTTP/1.1
Connection: Close
Host: 192.168.100.5
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

and received the following response from the remote server:

```
HTTP/1.1 200 OK
Date: Mon, 30 Mar 2020 07:55:59 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
TRACE /Nessus661699624.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.100.5
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```
85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy ‘frame-ancestors’ response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The ‘frame-ancestors’ policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56
https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the ‘frame-ancestors’ directive) HTTP header with the page’s response.

This prevents the page’s content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:693
Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/80

The following pages do not use a clickjacking mitigation response header and contain a clickable event:

- http://192.168.100.5/hca.html
Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2019/11/22

Plugin Output

tcp/80

```
URL : http://192.168.100.5/
Version : 2.2.99
backported : 1
```
**Synopsis**

This plugin determines which HTTP methods are allowed on various CGI directories.

**Description**

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
- PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

**See Also**

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2009/12/10, Modified: 2019/03/19

**Plugin Output**

tcp/80

---

Based on the response to an OPTIONS request:
- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on : 

    /

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPIY BDELETE BMOVE BPROPFIND
  BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
  LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
  ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
  RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
  UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on : 

    /

- Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
10107 - HTTP Server Type and Version

Synopsis
A web server is running on the remote host.

Description
This plugin attempts to determine the type and the version of the remote web server.

Solution
n/a

Risk Factor
None

Plugin Information
Published: 2000/01/04, Modified: 2019/11/22

Plugin Output
tcp/80

The remote web server type is :
Apache/2.2.21 (Unix) DAV/2
24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80

Response Code : HTTP/1.1 200 OK
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Mon, 30 Mar 2020 07:55:56 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Content-Length: 293
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /</title>
</head>
<body>
<ul>
<li><a href="cgi-bin/">cgi-bin/</a></li>
<li><a href="favicon.ico">favicon.ico</a></li>
<li><a href="hca.html">hca.html</a></li>
</ul>
Synopsis
The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description
The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also
http://www.nessus.org/u?55aa8f57
http://www.nessus.org/u?07cc2a06
https://content-security-policy.com/
https://www.w3.org/TR/CSP2/

Solution
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor
None

Plugin Information
Published: 2010/10/26, Modified: 2018/11/15

Plugin Output
tcp/80

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy:
- http://192.168.100.5/
- http://192.168.100.5/cgi-bin/vuln.cgi
- http://192.168.100.5/hca.html
**Synopsis**

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

**Description**

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

**See Also**

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

**Solution**

Set a properly configured X-Frame-Options header for all requested resources.

**Risk Factor**

None

**Plugin Information**

Published: 2010/10/26, Modified: 2017/05/16

**Plugin Output**

tcp/80

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- http://192.168.100.5/
- http://192.168.100.5/cgi-bin/vuln.cgi
- http://192.168.100.5/hca.html
11219 - Nessus SYN scanner

**Synopsis**

It is possible to determine which TCP ports are open.

**Description**

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Plugin Information**

Published: 2009/02/04, Modified: 2020/03/02

**Plugin Output**

tcp/22

Port 22/tcp was found to be open
**Synopsis**

It is possible to determine which TCP ports are open.

**Description**

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Plugin Information**

Published: 2009/02/04, Modified: 2020/03/02

**Plugin Output**

tcp/80

Port 80/tcp was found to be open
**19506 - Nessus Scan Information**

**Synopsis**

This plugin displays information about the Nessus scan.

**Description**

This plugin displays, for each tested host, information about the scan itself:

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2005/08/26, Modified: 2019/12/03

**Plugin Output**

tcp/0

Information about this scan:

Nessus version : 8.9.1
Plugin feed version : 202003280100
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Web Application Tests
Scanner IP : 192.168.100.4
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2020/3/30 3:55 EDT
Scan duration : 43 sec
91815 - Web Application Sitemap

**Synopsis**
The remote web server hosts linkable content that can be crawled by Nessus.

**Description**
The remote web server contains linkable content that can be used to gather information about a target.

**See Also**
http://www.nessus.org/u?5496c8d9

**Solution**
n/a

**Risk Factor**
None

**Plugin Information**
Published: 2016/06/24, Modified: 2016/06/24

**Plugin Output**
tcp/80

The following sitemap was created from crawling linkable content on the target host:
- http://192.168.100.5/
- http://192.168.100.5/cgi-bin/vuln.cgi
- http://192.168.100.5/favicon.ico
- http://192.168.100.5/hca.html

Attached is a copy of the sitemap file.
11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2018/11/15

Plugin Output

tcp/80

The following directories were discovered:
/cgi-bin

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards.
**Synopsis**

The remote server is running with WebDAV enabled.

**Description**

WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

**Solution**


**Risk Factor**

None

**Plugin Information**

Published: 2003/03/20, Modified: 2011/03/14

**Plugin Output**

tcp/80