Scan Report

December 29, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “DC$_{s}can''.Thescanstartedatandendedat.Th$

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.104	3	2	2	0	0
Total: 1	3	2	2	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 7 results selected by the filtering described above. Before filtering there were 109 results.

2 Results per Host

2.1 192.168.10.104

Host scan start
Host scan end

Service (Port)	Threat Level
general/tcp	High
80/tcp	High
22/tcp	Medium
80/tcp	Medium
22/tcp	Low
general/tcp	Low

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result

```
cpe:/o:debian:debian_linux:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪.105937)
```

Summary

OS End Of Life Detection.

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "Debian GNU/Linux" Operating System on the remote host has reached the end o
↪f life.
CPE:                cpe:/o:debian:debian_linux:7
Installed version,
build or SP:        7
EOL date:           2018-05-31
EOL info:           https://en.wikipedia.org/wiki/List_of_Debian_releases#Release
↪_table
```

Solution

Solution type: Mitigation

Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

Details: `OS End Of Life Detection`

OID:1.3.6.1.4.1.25623.1.0.103674

Version used: `2019-10-21T09:55:06+0000`

Product Detection Result

Product: `cpe:/o:debian:debian_linux:7`

Method: `OS Detection Consolidation and Reporting`

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.10.104]

2.1.2 High 80/tcp

High (CVSS: 7.5)

NVT: Drupal Core SQL Injection Vulnerability

Product detection result

```
cpe:/a:drupal:drupal:7
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Drupal is prone to an SQL-injection vulnerability

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Solution
Solution type: VendorFix
Updates are available

Affected Software/OS
Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight
Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method
Send a special crafted HTTP POST request and check the response.
Details: `Drupal Core SQL Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105101
Version used: `$Revision: 13659 $`

Product Detection Result
Product: `cpe:/a:drupal:drupal:7`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References
```
CVE: CVE-2014-3704
BID:70595
Other:
  URL:http://www.securityfocus.com/bid/70595
   URL:http://drupal.org/
```

High (CVSS: 7.5)
NVT: Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Active Check)

Product detection result
```
cpe:/a:drupal:drupal:7
Detected by Drupal Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100169)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

This host is running Drupal and is prone to critical remote code execution vulnerability.

Vulnerability Detection Result

```
By doing the following subsequent requests:
Req 1: "HTTP POST" body  : form_id=user_pass&_triggering_element_name=name
Req 1: URL               : http://192.168.10.104/?q=user%2Fpassword&name%5B%23po
↪st_render%5D%5B%5D=printf&name%5B%23markup%5D=Y90l0dc_HMoLQXD8&name%5B%23typ
Req 2: "HTTP POST" body  : form_build_id=form-vBF_e13QLbvI65DmjrR_LqNYCxyB6cR-Sp
↪P64aJIoPA
Req 2: URL               : http://192.168.10.104/?q=file%2Fajax%2Fname%2F%23valu
↪e%2Fform-vBF_e13QLbvI65DmjrR_LqNYCxyB6cR-SpP64aJIoPA
it was possible to execute the "printf" command to return the data "Y90l0dc_HMoL
↪QXD8".
Result:
Y90l0dc_HMoLQXD8[{"command":"settings","settings":{"basePath":"\/","pathPrefix":
↪"","ajaxPageState":{"theme":"bartik","theme_token":"TFUbkq2LeYVBxfBMZOWulv1puS
↪9imYPwTnRmg31wLkw"}},"merge":true},{"command":"insert","method":"replaceWith",
↪"selector":null,"data":"\u003Cdiv class=\u0022messages error\u0022\u003E
\u003Ch2 class=\u0022element-invisible\u0022\u003EError message\u003C\/h2\u003E
 \u003Cul\u003E
  \u003Cli\u003E\u003Cem class=\u0022placeholder\u0022\u003ENotice\u003C\/em\u00
↪3E: Undefined index: #value in \u003Cem class=\u0022placeholder\u0022\u003Efil
↪e_ajax_upload()\u003C\/em\u003E (line \u003Cem class=\u0022placeholder\u0022\u
↪003E262\u003C\/em\u003E of \u003Cem class=\u0022placeholder\u0022\u003E\/var\/
↪www\/modules\/file\/file.module\u003C\/em\u003E).\u003C\/li\u003E
  \u003Cli\u003E\u003Cem class=\u0022placeholder\u0022\u003ENotice\u003C\/em\u00
↪3E: Undefined index: #suffix in \u003Cem class=\u0022placeholder\u0022\u003Efi
↪le_ajax_upload()\u003C\/em\u003E (line \u003Cem class=\u0022placeholder\u0022\
↪u003E280\u003C\/em\u003E of \u003Cem class=\u0022placeholder\u0022\u003E\/var\
↪/www\/modules\/file\/file.module\u003C\/em\u003E).\u003C\/li\u003E
 \u003C\/ul\u003E
\u003C\/div\u003E
16\u003Cspan class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settin
↪gs":{"basePath":"\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_
↪token":"TFUbkq2LeYVBxfBMZOWulv1puS9imYPwTnRmg31wLkw"}}}]
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code and completely compromise the site.

Solution

Solution type: VendorFix

Upgrade to Drupal core version 8.3.9 or 8.4.6 or 8.5.1 or 7.58 later. Please see the refereced links for available updates.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Drupal core versions 6.x and earlier,
Drupal core versions 8.2.x and earlier,
Drupal core versions 8.3.x to before 8.3.9,
Drupal core versions 8.4.x to before 8.4.6,
Drupal core versions 8.5.x to before 8.5.1 and
Drupal core versions 7.x to before 7.58 on Windows.

Vulnerability Insight

The flaw exists within multiple subsystems of Drupal. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

Vulnerability Detection Method

Send a crafted HTTP POST request and check the response.
Details: `Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Ac.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108438
Version used: `$Revision: 14034 $`

Product Detection Result

Product: `cpe:/a:drupal:drupal:7`
Method: `Drupal Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.100169)

References

```
CVE: CVE-2018-7600
Other:
  URL:https://www.drupal.org/psa-2018-001
   URL:https://www.drupal.org/sa-core-2018-002
   URL:https://www.drupal.org/project/drupal/releases/7.58
   URL:https://www.drupal.org/project/drupal/releases/8.3.9
   URL:https://www.drupal.org/project/drupal/releases/8.4.6
   URL:https://www.drupal.org/project/drupal/releases/8.5.1
   URL:https://research.checkpoint.com/uncovering-drupalgeddon-2/
```

[return to 192.168.10.104]

2.1.3 Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.

Vulnerability Insight

The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: `SSH Weak Encryption Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105611

Version used: `$Revision: 13581 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
Other:
  URL:https://tools.ietf.org/html/rfc4253#section-6.3
   URL:https://www.kb.cert.org/vuls/id/958563
```

[return to 192.168.10.104]

2.1.4 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.10.104/:pass
http://192.168.10.104/user:pass
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `$Revision: 10726 $`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

[return to 192.168.10.104]

2.1.5 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary

The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

Solution

Solution type: Mitigation

Disable the weak MAC algorithms.

Vulnerability Detection Method

Details: `SSH Weak MAC Algorithms Supported`

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: `$Revision: 13581 $`

[return to 192.168.10.104]

2.1.6 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 229384
Packet 2: 229656
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 192.168.10.104]

This file was automatically generated.