Scan Report

June 16, 2023

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 "648bd53dd919bf500bdc587d-648bd53dd919bf500bdc58cb-7e666944". The scan started at Fri Jun 16 03:22:01 2023 UTC and ended at Fri Jun 16 04:01:18 2023 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
20.223.224.66 diplomasite.northeurope.cloudapp.azure.com	0	1	1	27	0
Total: 1	0	1	1	27	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.
Only results with a minimum QoD of 70 are shown.

This report contains all 29 results selected by the filtering described above. Before filtering there were 29 results.

2 Results per Host

2.1 20.223.224.66

Host scan start	Fri Jun 16 03:22:32 2023 UTC
Host scan end	Fri Jun 16 04:01:14 2023 UTC

Service (Port)	Threat Level
443/tcp	Medium
general/tcp	Low
general/tcp	Log
443/tcp	Log
80/tcp	Log

2.1.1 Medium 443/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
`In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and`

... continues on next page ...

... continued from previous page ...

↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: 2021-07-19T08:11:48Z

References
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2011-1482

[return to 20.223.224.66]

2.1.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

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/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 734741075
Packet 2: 1944538989

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 implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2023-05-11T09:09:33Z

... continues on next page ...

... continued from previous page ...

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152

[return to 20.223.224.66]

2.1.3 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Vulnerability Detection Result
Hostname determination for IP 20.223.224.66:
Hostname|Source
20.223.224.66|IP-address

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community forum.

Vulnerability Detection Result
No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner
↪ Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify
↪this OS.

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2023-06-06T09:09:18Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result
```
The following additional and resolvable hostnames were detected:
diplomasite.northeurope.cloudapp.azure.com
```

Solution:

Log Method
Details: `SSL/TLS: Hostname discovery from server certificate`
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: `2021-11-22T15:32:39Z`

Log (CVSS: 0.0)
NVT: Traceroute

Summary
Collect information about the network route and network distance between the scanner host and the target host.

Vulnerability Detection Result
```
Network route from scanner (10.88.0.2) to target (20.223.224.66):
10.88.0.2
10.206.6.27
10.206.35.19
10.206.32.2
173.255.239.101
```

... continues on next page ...

... continued from previous page ...

```
23.203.156.50
62.115.171.40
62.115.161.51
104.44.43.105
104.44.33.211
104.44.17.153
104.44.28.124
104.44.23.157
104.44.21.217
104.44.17.155
104.44.23.155
20.223.224.66
Network distance between scanner and target: 17
```

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `2022-10-17T11:13:19Z`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community forum.

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: Server: Microsoft-Azure-Application-Gateway/v2
Identified from: HTTP Server banner on port 443/tcp
```

... continues on next page ...

... continued from previous page ...

Banner: Server: Microsoft-Azure-Application-Gateway/v2
Identified from: HTTP Server banner on port 80/tcp

Solution:

Log Method
Details: Unknown OS and Service Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: 2022-09-22T10:44:54Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

[return to 20.223.224.66]

2.1.4 Log 443/tcp

Log (CVSS: 0.0)
NVT: Anti-Scanner Defenses (HTTP)

Summary
It seems that the remote web server rejects HTTP requests from the Scanner. It is probably protected by a reverse proxy, WAF or IDS/IPS.

Vulnerability Detection Result
By sending a different User-Agent the remote web server is answering with differ
↪ent HTTP responses:
1. Status Code : 502
1. User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
↪HTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393
2. Status Code : 403
2. User-Agent : Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)

Solution:
Whitelist the IP of the scanner to e.g. not block/reject HTTP requests done by scanner for accurate audit/scan results.

Log Method
Details: Anti-Scanner Defenses (HTTP)
OID:1.3.6.1.4.1.25623.1.0.11238
Version used: 2023-04-27T12:17:38Z

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community forum.

Vulnerability Detection Result
```
The Hostname/IP "20.223.224.66" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
https://20.223.224.66/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2023-03-06T10:19:58Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
```

... continues on next page ...

... continued from previous page ...

```
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                                   | Enumeration technique
--------------------------------------------------------------------------------
↪---------------------------------
Server: Microsoft-Azure-Application-Gateway/v2 | Invalid HTTP 00.5 GET request (
↪non-existent HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: Microsoft-Azure-Application-Gateway/v2

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-08-24T15:18:35Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Vulnerability Detection Result
`A web server is running on this port through SSL`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | F91147BF1FA3F63EBC01085DCFBB2EB7F5D1AC02
fingerprint (SHA-256)           | C2C7E0636FC22EDFD3F08AC8202AC6705C8FB374080E02
↪20EEC82FE25B0AFC7E
issued by                       | CN=R3,O=Let's Encrypt,C=US
public key size (bits)          | 256
serial                          | 04429E8462AB170F78C0FA7694CB2A0EF581
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=diplomasite.northeurope.cloudapp.azure.com
subject alternative names (SAN) | diplomasite.northeurope.cloudapp.azure.com
valid from                      | 2023-06-15 14:44:36 UTC
valid until                     | 2023-09-13 14:44:35 UTC
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2023-02-17T10:19:33Z

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
The remote web server is not enforcing HPKP.
Note: Most major browsers have dropped / deprecated support for this header in 2020.

Vulnerability Detection Result
```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Server: Microsoft-Azure-Application-Gateway/v2
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
```

Solution:
Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2021-01-26T13:20:44Z

References
```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-
↪for-http-hpkp
url: https://tools.ietf.org/html/rfc7469
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
```

... continues on next page ...

... continued from previous page ...

url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HSTS.

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Server: Microsoft-Azure-Application-Gateway/v2
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
```

Solution:
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code.
- Apache: Use 'Header always set' instead of 'Header set'.
- nginx: Append the 'always' keyword to each 'add_header' directive.
For different applications or web severs please refer to the related documentation for a similar configuration possibility.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2021-01-26T13:20:44Z

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).
Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Vulnerability Detection Result
```
The remote service advertises support for the following Network Protocol(s) via
↪the NPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.0:HTTP/1.1
TLSv1.1:HTTP/1.1
TLSv1.2:HTTP/1.1
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.0:HTTP/1.1
TLSv1.1:HTTP/1.1
TLSv1.2:HTTP/1.1
```

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2023-04-18T10:19:20Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
```

... continues on next page ...

... continued from previous page ...

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2021-12-01T13:10:37Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2021-12-01T09:24:41Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result
```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.1 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2021-12-09T13:40:52Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
```

... continues on next page ...

... continued from previous page ...

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.
```

Solution:

Vulnerability Insight
Notes:
- As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.
- SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2022-08-25T10:12:37Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
The remote SSL/TLS service supports the following SSL/TLS protocol version(s):
TLSv1.0
TLSv1.1
TLSv1.2
```

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2021-12-06T15:42:24Z`

[return to 20.223.224.66]

2.1.5 Log 80/tcp

Log (CVSS: 0.0)
NVT: Anti-Scanner Defenses (HTTP)

Summary
It seems that the remote web server rejects HTTP requests from the Scanner. It is probably protected by a reverse proxy, WAF or IDS/IPS.

Vulnerability Detection Result

```
By sending a different User-Agent the remote web server is answering with differ
↪ent HTTP responses:
1. Status Code : 200
1. User-Agent  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
↪HTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393
2. Status Code : 403
2. User-Agent  : Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)
```

Solution:
Whitelist the IP of the scanner to e.g. not block/reject HTTP requests done by scanner for accurate audit/scan results.

Log Method
Details: `Anti-Scanner Defenses (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11238
Version used: `2023-04-27T12:17:38Z`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community forum.

Vulnerability Detection Result
```
The Hostname/IP "20.223.224.66" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://20.223.224.66/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `CGI Scanning Consolidation`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2023-03-06T10:19:58Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
```

... continues on next page ...

... continued from previous page ...

X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result
It was possible to enumerate the following HTTP server banner(s):

Server banner	Enumeration technique
Server: Microsoft-Azure-Application-Gateway/v2	Invalid HTTP 00.5 GET request (non-existent HTTP version) to '/'

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

... continues on next page ...

... continued from previous page ...

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: Microsoft-Azure-Application-Gateway/v2`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2020-08-24T15:18:35Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 20.223.224.66]