Scan Report

January 9, 2020

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 "Immediate scan of IP b24.reaspekt.ru". The scan started at Thu Jan 9 16:24:29 2020 UTC and ended at Thu Jan 9 16:38:09 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 2

2 Results per Host 2

2.1 92.53.96.138 . . . 2

2.1.1 Medium 443/tcp . . . 2

2.1.2 Medium 21/tcp . . . 4

2.1.3 Medium 80/tcp . . . 5

2.1.4 Medium 22/tcp . . . 5

2.1.5 Low 22/tcp . . . 7

2.1.6 Low general/tcp . . . 8

Result Overview

Host	High	Medium	Low	Log	False Positive
92.53.96.138 b24.reaspekt.ru	0	5	2	0	0
Total: 1	0	5	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 61 results.

Results per Host

92.53.96.138

Host scan start	Thu Jan 9 16:24:34 2020 UTC
Host scan end	Thu Jan 9 16:38:09 2020 UTC

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

Medium 443/tcp

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing 'secure' Cookie Attribute

Summary
The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/
are missing the "secure" attribute.
```

Solution

Solution type: Mitigation

Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Affected Software/OS

Server with SSL/TLS.

Vulnerability Insight

The flaw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Vulnerability Detection Method

Details: `SSL/TLS: Missing ‘secure‘ Cookie Attribute`

OID:1.3.6.1.4.1.25623.1.0.902661

Version used: `$Revision: 11374 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/SecureFlag
   URL:http://www.ietf.org/rfc/rfc2965.txt
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-
↪002)
```

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: PHPSESSID=***replaced***; path=/
are missing the "httpOnly" attribute.
```

Solution

Solution type: Mitigation

Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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

Version used: `$Revision: 5270 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

[return to 92.53.96.138]

Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Anonymous sessions:     331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.
```

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `$Revision: 13611 $`

[return to 92.53.96.138]

Medium 80/tcp

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: PHPSESSID=***replaced***; 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
Version used: `$Revision: 5270 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

[return to 92.53.96.138]

Medium 22/tcp

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

Summary
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`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `$Revision: 13581 $`

References

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

[return to 92.53.96.138]

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-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

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 92.53.96.138]

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: 3414365662
Packet 2: 3414366799
```

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 92.53.96.138]