FortiGate 6.4.5 – 192.168.217.100

Report generated by Tenable Nessus™ Sat, 19 Oct 2024 23:26:10 Egypt Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.217.100

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	20	37	7	32

Host Information

IP:	192.168.217.100
MAC Address:	00:0C:29:EF:42:28
OS:	FortiOS 6.4.5,build1828,210217 on FortiGate-VM64

Vulnerabilities

156752 - Fortinet FortiOS Integer Overflow (FG-IR-21-049)

Synopsis

The remote host is affected by a integer overflow vulnerability.

Description

The remote host is running a version of FortiOS prior or equal to 6.0.12, 6.2.x prior or equal to 6.2.9, 6.4.x prior or equal to 6.4.5 or 7.0.0. It is, therefore, affected by an integer overflow vulnerability in FortiOS SSLVPN memory allocator may allow an unauthenticated attacker to corrupt control data on the heap via specifically crafted requests to SSLVPN, resulting in potentially arbitrary code execution.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-049

Solution

See vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0029

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-26109
XREF	IAVA:2021-A-0574-S

Plugin Information

Published: 2022/01/14, Modified: 2022/09/19

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.6
```

172390 - Fortinet Fortigate - Heap buffer underflow in administrative interface (FG-IR-23-001)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-001 advisory.

- A buffer underflow vulnerability in FortiOS & FortiProxy HTTP/HTTPS administrative interface could allow an unauthenticated, remote attacker to execute arbitrary code on the device and/or perform a DoS using specifically crafted requests. (CVE-2023-25610)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-001

Solution

Upgrade to Fortigate version 6.2.13 / 6.4.12 / 7.0.10 / 7.2.4 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-25610
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2023/03/09, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

179479 - Fortinet Fortigate - SSH authentication bypass when RADIUS authentication is used (FG-IR-22-255)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-255 advisory.

- An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access- Challenge response from the Radius server. (CVE-2022-35843)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-255

Solution

Please upgrade to FortiOS version 7.2.2 or above Please upgrade to FortiOS version 7.0.8 or above Please upgrade to FortiOS version 6.4.10 or above Please upgrade to upcoming FortiOS version 6.2.13 or above Please upgrade to FortiProxy version 7.0.7 or above Please upgrade to FortiProxy version 2.0.11 or above

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.002

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2022-35843
XREF	IAVA:2022-A-0458-S

Plugin Information

Published: 2023/08/08, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.10
```

172579 - Fortinet FortiOS - Path Traversal Vulnerability (FG-IR-22-401)

Synopsis

Fortinet Firewall is affected by a privilege escalation.

Description

The version of FortiOS installed on the remote host is affected by a path traversal vulnerability. A relative path traversal vulnerability [CWE-23] in FortiOS and FortiProxy may allow privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-401

Solution

Upgrade to Fortigate version 6.2.13 / 6.4.12 / 7.0.9 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.2 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-42476
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2023/03/15, Modified: 2023/04/13

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

172491 - Fortinet FortiOS - Path Traversal in Execute Command (FG-IR-22-369)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of FortiOS installed on the remote host is therefore, affected by a path traversal in execute command vulnerability. A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') in FortiOS may allow a privileged attacker to read and write arbitrary files via crafted CLI commands.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-369

Solution

Upgrade to Fortigate version to 6.2.14 / 6.4.12 / 7.0.10 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.1103

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-41328
XREF	IAVA:2023-A-0125-S
XREF	CISA-KNOWN-EXPLOITED:2023/04/04

Plugin Information

Published: 2023/03/13, Modified: 2023/08/09

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

161892 - Fortinet FortiOS < 6.0.14 / 6.2 < 6.2.10 / 6.4 < 6.4.8 / 7.0 < 7.0.3 Arbitrary File Download (FG-IR-21-201)

Synopsis

The remote host is affected by an arbitrary file download.

Description

The remote host is running a version of FortiOS prior to 6.0.14, 6.2 prior to 6.2.10, 6.4 prior to 6.4.8, or 7.0 prior to 7.0.3.

It is, therefore, affected by an arbitrary file download vulnerability that could allow a local authenticated attacker to download arbitrary files on the device via specially crafted update packages.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://fortiguard.com/psirt/FG-IR-21-201

Solution

Upgrade to Fortinet FortiOS version to 6.0.14, 6.2.10, 6.4.8, 7.0.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-44168
XREF	CISA-KNOWN-EXPLOITED:2021/12/24

Plugin Information

Published: 2022/06/06, Modified: 2023/04/25

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.8
```

152514 - Fortinet FortiOS <= 6.2.9 / 6.4.x <= 6.4.6 / 7.0.0 Buffer Underwrite (FG-IR-21-046)

Synopsis

The remote host is affected by a buffer underwrite vulnerability.

Description

The remote host is running a version of FortiOS prior or equal to 6.2.9 or 6.4.x prior or equal to 6.4.6 or 7.0.0. It is, therefore, affected by a buffer underwriter vulnerability in the firmware verification routine of FortiOS that may allow an attacker located in the adjacent network to potentially execute arbitrary code via a specifically crafted firmware image.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-046

Solution

Upgrade to Fortinet FortiOS version 6.2.10 / 6.4.7 / 7.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-24018
XREF	IAVA:2021-A-0368-S

Plugin Information

Published: 2021/08/12, Modified: 2022/09/16

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.7
```

156755 - Fortinet FortiOS Hard-Coded Cryptographic Key (FG-IR-21-051)

Synopsis

The remote host is affected by a hard-coded cryptographic key vulnerability.

Description

The remote host is running a version of FortiOS prior to 5.6.13, 6.0.x prior or equal to 6.0.12, 6.2.x prior or equal to 6.2.8, or 6.4.x prior or equal to 6.4.5, FortiOS-6K7K version prior to 6.2.6 and 6.4.2. It is, therefore, affected by a hard-coded cryptographic key vulnerability in FortiOS SSLVPN may allow an attacker to retrieve the key by reverse engineering.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-051

Solution

See vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0017

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-26108
XREF	IAVA:2021-A-0574-S

Plugin Information

Published: 2022/01/14, Modified: 2022/09/19

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.6
```

156783 - Fortinet FortiOS Privilege Escalation (FG-IR-20-131)

Synopsis

The remote host is affected by a privilege escalation vulnerability.

Description

The remote host is running a version of FortiOS prior or equal to 6.0.12, 6.2.x prior or equal to 6.2.9, 6.4.x prior or equal to 6.4.6, 7.0.0 or FortiOS-6K7K version prior or equal to 6.2.6, 6.4.2. It is, therefore, affected by a privilege escalation vulnerability in FortiOS autod daemon, which may allow an authenticated low-privileged attacker to escalate their privileges to super_admin via a specific crafted configuration of fabric automation CLI script and auto-script features.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-20-131

Solution

See vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-26110
XREF	IAVA:2021-A-0574-S

Plugin Information

Published: 2022/01/18, Modified: 2022/09/19

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.7
```

166981 - Fortinet FortiOS SSL-VPN Information Disclosure (FG-IR-21-223)

Synopsis

The remote host is affected by an information disclosure vulnerability.

Description

The remote host is running a version of FortiOS that is 6.4.x through 6.4.9, or 7.0.x through 7.0.7, or 7.2.0. It is, therefore, affected by an information disclosure vulnerability in the SSL_VPN. An unauthenticated, remote attacker can exploit this, to disclose potentially sensitive information.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-223

Solution

Update FortiOS to version 6.4.10, 7.0.7, 7.2.2, or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.002

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2022-35842
XREF	IAVA:2022-A-0458-S
XREF	CWE:200

Plugin Information

Published: 2022/11/04, Modified: 2023/02/24

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.10
```

205439 - Fortinet Fortigate (FG-IR-22-445)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-445 advisory.

- An insufficient session expiration vulnerability [CWE-613] in FortiOS, FortiProxy, FortiPAM &

FortiSwitchManager GUI may allow attackers to re-use websessions after GUI logout, should they manage to acquire the required credentials. (CVE-2022-45862)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-445

Solution

Upgrade to Fortigate version 6.4.999999 / 7.0.999999 / 7.2.6 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-45862
XREF	IAVA:2024-A-0381
XREF	IAVA:2024-A-0165
XREF	IAVA:2024-A-0514

Plugin Information

Published: 2024/08/13, Modified: 2024/08/23

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : See vendor advisory
```

200328 - Fortinet Fortigate (FG-IR-23-460)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-460 advisory.

- A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0 all versions allows attacker to execute unauthorized code or commands via specially crafted commands (CVE-2024-23110)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-460

Solution

Upgrade to Fortigate version 6.0.999999 / 6.2.16 / 6.4.15 / 7.0.14 / 7.2.7 / 7.4.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-23110

Plugin Information

Published: 2024/06/11, Modified: 2024/06/11

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.15
```

197606 - Fortinet Fortigate (FG-IR-23-493)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-493 advisory.

- A insufficiently protected credentials in Fortinet FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17 allows attacker to execute unauthorized code or commands via targeted social engineering attack (CVE-2023-41677)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-493

Solution

Upgrade to Fortigate version 6.2.16 / 6.4.15 / 7.0.13 / 7.2.7 / 7.4.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-41677
XREF	IAVA:2024-A-0165

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.15
```

174262 - Fortinet Fortigate - Anti brute-force bypass in administrative interface (FG-IR-22-444)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-444 advisory.

- An improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiOS version 7.2.0 through 7.2.3 and before 7.0.10, FortiProxy version 7.2.0 through 7.2.2 and before 7.0.8 administrative interface allows an attacker with a valid user account to perform brute-force attacks on other user accounts via injecting valid login sessions. (CVE-2022-43947)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-444

Solution

Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.11 or above Please upgrade to FortiOS version 6.4.13 or above

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-43947
XREF	IAVA:2023-A-0198-S

Plugin Information

Published: 2023/04/13, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

171852 - Fortinet Fortigate - Arbitrary read/write vulnerability in administrative interface (FG-IR-22-391)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-391 advisory.

- A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.10, FortiProxy version 7.2.0 through 7.2.1, 7.0.0 through 7.0.7 and before 2.0.10, FortiSwitchManager 7.2.0 and before 7.0.0 allows an authenticated attacker to read and write files on the underlying Linux system via crafted HTTP requests. (CVE-2022-41335)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-391

Solution

Upgrade to Fortigate version 6.2.13 / 6.4.11 / 7.0.9 / 7.2.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-41335

Plugin Information

Published: 2023/02/23, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.11
```

177125 - Fortinet Fortigate - Format String Bug in Fclicense daemon (FG-IR-23-119)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-119 advisory.

- A use of externally-controlled format string in Fortinet FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted command. (CVE-2023-29181)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-119

Solution

Please upgrade to FortiOS version 7.4.0 or above

Please upgrade to FortiOS version 7.2.5 or above

Please upgrade to FortiOS version 7.0.12 or above

Please upgrade to FortiOS version 6.4.13 or above

Please upgrade to FortiOS version 6.2.15 or above

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-29181
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

174403 - Fortinet Fortigate - Lack of certificate verification when establishing secure connections with threat feed fabric connectors (FG-IR-22-257)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-257 advisory.

- An improper certificate validation vulnerability [CWE-295] in FortiOS 7.2.0 through 7.2.3, 7.0.0 through 7.0.7, 6.4 all versions, 6.2 all versions, 6.0 all versions and FortiProxy 7.0.0 through 7.0.6, 2.0 all versions, 1.2 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the FortiOS/FortiProxy device and remote servers hosting threat feeds (when the latter are configured as Fabric connectors in FortiOS/FortiProxy) (CVE-2022-39948)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-257

Solution

Please upgrade to FortiProxy version 7.2.0 or above Please upgrade to FortiProxy version 7.0.7 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.8 or above

Risk Factor

High

CVSS v3.0 Base Score

7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

EPSS Score

0.0009

CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-39948
XREF	IAVA:2023-A-0110-S

Plugin Information

Published: 2023/04/17, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.8
```

177122 - Fortinet Fortigate - Null pointer dereference in sslvnd (FG-IR-23-111)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-111 advisory.

- A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.3, 7.0.0 through 7.0.10, 2.0.0 through 2.0.12, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to denial of service via specially crafted HTTP requests. (CVE-2023-29180)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-111

Solution

Please upgrade to FortiOS version 7.4.0 or above

Please upgrade to FortiOS version 7.2.5 or above

Please upgrade to FortiOS version 7.0.12 or above

Please upgrade to FortiOS version 6.4.13 or above

Please upgrade to FortiOS version 6.2.15 or above

Please upgrade to FortiOS version 6.0.17 or above

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-29180
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

177127 - Fortinet Fortigate - Out-of-bound write in CLI (FG-IR-22-494)

Synopsis

Fortinet Firewall is affected by a privilege escalation.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-494 advisory.

- A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows attacker to escalation of privilege via specifically crafted commands. (CVE-2023-22639)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-494

Solution

Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.11 or above Please upgrade to FortiOS version 6.4.13 or above Please upgrade to FortiProxy version 7.2.3 or above Please upgrade to FortiProxy version 7.0.9 or above

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-22639
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

197615 - Fortinet Fortigate - Path traversal in execute command (FG-IR-22-369)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-369 advisory.

- A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via crafted CLI commands. (CVE-2022-41328)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-369

Solution

Upgrade to Fortigate version 6.4.12 / 7.0.10 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.1103

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-41328
XREF	CISA-KNOWN-EXPLOITED:2023/04/04
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

197604 - Fortinet Fortigate - Path traversal vulnerability allows VDOM escaping (FG-IR-22-401)

Synopsis

Fortinet Firewall is affected by a privilege escalation.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-401 advisory.

- A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.11, FortiProxy version 7.2.0 through 7.2.2 and 7.0.0 through 7.0.8 allows privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests. (CVE-2022-42476)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-401

Solution

Upgrade to Fortigate version 6.2.13 / 6.4.12 / 7.0.9 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

8.2 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-42476
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

165982 - Fortinet Fortigate - Privilege escalation via switch-control CLI command (FG-IR-21-242)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-21-242 advisory.

- Animproper neutralization of special elements used in an os command [CWE-78] vulnerability in FortiOSmay allow an authenticated attacker to execute privileged commands on a linked FortiSwitch via diagnostic CLI commands. (CVE-2021-44171)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Fortigate version 6.0.15 / 6.2.11 / 6.4.9 / 7.0.7 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.0 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

7.7 (CVSS2#AV:A/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-44171
XREF	IAVA:2022-A-0401-S

Plugin Information

Published: 2022/10/10, Modified: 2023/02/24

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

177126 - Fortinet Fortigate -resources CLI command (FG-IR-22-463)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-463 advisory.

- A use of externally-controlled format string in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS all versions 7.0, FortiOS all versions 6.4, FortiOS all versions 6.2, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7 allows attacker to execute unauthorized code or commands via specially crafted commands. (CVE-2022-43953)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-463

Solution

Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.5 or above Please upgrade to FortiOS version 7.0.12 or above Please upgrade to FortiOS version 6.4.13 or above

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-43953
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

150156 - Fortinet FortiGate <= 5.6.13 / 6.0.x < 6.0.13 / 6.2.x < 6.2.8 / 6.4.x < 6.4.5 XSS (FG-IR-20-199)

Synopsis

The remote host is affected by a cross-site scripting vulnerability.

Description

The remote host is running a FortiOS version prior or equal to 5.6.13, 6.0.x prior to 6.0.13, 6.2.x prior to 6.2.8, or 6.4.x prior to 6.4.6. It is, therefore, affected by a cross-site scripting vulnerability. An unauthenticated attacker may be able perform a reflected cross-site scripting attack by sending a request to the error page with malicious GET parameters.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-20-199

Solution

Upgrade to Fortinet FortiOS version 6.0.13, 6.2.8, 6.4.6, 7.0.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-26092
XREF	IAVA:2021-A-0262

Plugin Information

Published: 2021/06/03, Modified: 2022/09/16

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.6
```

172492 - Fortinet FortiOS - Information Disclosure (FG-IR-22-364)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of FortiOS installed on the remote host is therefore, affected by a information disclosure vulnerability. An exposure of sensitive information to an unauthorized actor vulnerability in FortiOS and FortiProxy may allow an unauthenticated attacker to obtain sensitive logging information on the device via crafted HTTP GET requests.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-364

Solution

Upgrade to Fortigate version 6.4.12 / 7.0.10 / 7.2.4 or later.

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)

VPR Score

1.4

EPSS Score

0.0018

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-41329
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2023/03/13, Modified: 2023/04/13

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

163252 - Fortinet FortiOS 7.0.x <= 7.0.5 / 6.4.x <= 6.4.9 XSS (FG-IR-21-057)

Synopsis

The remote host is affected by a cross-site scripting vulnerability.

Description

The remote host is running a version of FortiOS that is 7.0.x through 7.0.5 or 6.4.x through 6.4.9. It is, therefore, affected by a cross-site scripting (XSS) vulnerability due to improper neutralization of input during web page generation. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-057

Solution

Update FortiOS to version 7.0.6, 7.2.0, or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-23438
XREF	IAVA:2022-A-0264-S

Plugin Information

Published: 2022/07/15, Modified: 2022/12/08

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.6 / 7.2.0
```

132317 - Fortinet FortiOS < 5.6.10 / 6.0 < 6.0.7 / 6.2.x < 6.2.1 Vulnerable Encryption (FG-IR-19-007)

Synopsis

The remote host is running a version of FortiOS that has not yet enabled private data encryption.

Description

The remote host is running a version of FortiOS that has not yet enabled private-data-encryption. A authorized remote user with access or knowledge of the standard encryption key could gain access and decrypt the FortiOS backup files and all non-administor passwords and private keys.' (CVE-2019-6693)

See Also

https://fortiguard.com/psirt/FG-IR-19-007

Solution

Ensure that Fortinet FortiOS has been updated to 5.6.10, 6.0.7, 6.2.1, or later.

Additionally the user will need to set the private-data-encryption attribute based on instructions contained in FG-IR-19-007 advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0008

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-6693

Plugin Information

Published: 2019/12/19, Modified: 2024/02/12

Plugin Output

tcp/0

```
FortiOS is currently running a vulnerable configuration,
Based on private-data-encryption is currently not enabled.
Please ensure private-data-encryption is enabled.
```

161659 - Fortinet FortiOS Access Control (FG-IR-21-147)

Synopsis

The remote host is affected by a access control vulnerability.

Description

An improper access control vulnerability in FortiOS versions 6.4.8 and prior and 7.0.3 and prior may allow an authenticated attacker with a restricted user profile to gather sensitive information and modify the SSL-VPN tunnel status of other VDOMs using specific CLI commands.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-147

Solution

See vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.5

EPSS Score

0.0005

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2021-41032
XREF	IAVA:2022-A-0221-S

Plugin Information

Published: 2022/05/30, Modified: 2023/02/23

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

156569 - Fortinet FortiOS Buffer Overflow (FG-IR-21-173)

Synopsis

The remote host is affected by a buffer overflow vulnerability.

Description

The remote host is running a version of FortiOS prior to 6.0.13, 6.2.x prior or equal to 6.2.9, 6.4.x prior or equal to 6.4.7, 7.0.x prior or equal to 7.0.2 or FortiOS-6K7K version prior to 6.2.8. It is, therefore, affected by a buffer overflow vulnerability in the TFTP client library of FortiOS, may allow an authenticated local attacker to achieve arbitrary code execution via specially crafted command line arguments.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-173

Solution

See vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-42757
XREF	IAVA:2021-A-0574-S

Plugin Information

Published: 2022/01/10, Modified: 2022/09/19

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.8
```

163253 - Fortinet FortiOS Buffer Overflow (FG-IR-21-206)

Synopsis

The remote host is affected by a buffer overflow vulnerability.

Description

The remote host is running a version of FortiOS that is 6.0.x through 6.0.14, 6.2.x through 6.2.10, 6.4.x through 6.4.8, or 7.0.x through 7.0.5. It is, therefore, affected by a buffer overflow vulnerability. An authenticated, remote attacker can exploit this issue, via the TFTP protocol with crafted CLI 'execute restore image' and 'execute certificate remote' operations, to execute arbitrary code or commands in the system.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-206

Solution

Update FortiOS to version 6.2.11, 6.4.9, 7.0.6, 7.2.0, or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-43072
XREF	IAVA:2022-A-0264-S

Plugin Information

Published: 2022/07/15, Modified: 2023/10/17

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

163262 - Fortinet FortiOS Buffer Overflow (FG-IR-21-206)

Synopsis

The remote host is affected by a buffer overflow vulnerability.

Description

The remote host is running a version of FortiOS that is 6.0.x through 6.0.14, 6.2.x through 6.2.10, 6.4.x through 6.4.8, or 7.0.x through 7.0.2. It is, therefore, affected by a stack-based buffer overflow vulnerability. An authenticated, remote attacker can exploit this issue, via specially crafted command line arguments, to execute unauthorized code or commands.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-179

Solution

Update FortiOS to version 6.2.11, 6.4.9, 7.0.4, or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-44170
XREF	IAVA:2022-A-0264-S

Plugin Information

Published: 2022/07/15, Modified: 2022/12/08

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

161660 - Fortinet FortiOS Certificate Validation (FG-IR-21-239)

Synopsis

The remote host is affected by a certificate validation vulnerability.

Description

An improper certificate validation vulnerability in FortiOS 6.0.0 through 6.0.14, 6.2.0 through 6.2.10, 6.4.0 through 6.4.8, 7.0.0 may allow a network adjacent and unauthenticated attacker to man-in-the-middle the communication between the FortiGate and some peers such as private SDNs and external cloud platforms.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-239

Solution

See vendor advisory.

Risk Factor

Low

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2022-22306
XREF	IAVA:2022-A-0221-S

Plugin Information

Published: 2022/05/30, Modified: 2023/05/24

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

162782 - Fortinet FortiOS Integer Overflow (FG-IR-21-155)

Synopsis

The remote host is affected by an integer overflow vulnerability.

Description

An integer overflow vulnerability in the dhcpd daemon of FortiOS allows unauthenticated, adjacent attackers to cause a denial of service (DoS) condition.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-155

Solution

Update to FortiOS version 6.2.11, 6.49., 7.0.4 or later

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-42755
XREF	IAVA:2022-A-0264-S

Plugin Information

Published: 2022/07/07, Modified: 2023/05/24

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

161606 - Fortinet FortiOS Sensitive Information Disclosure (FG-IR-21-231)

Synopsis

The remote host is affected by a sensitive information vulnerability.

Description

A server-generated error message containing sensitive information in Fortinet FortiOS versions prior to 6.0, 6.2 to 6.2.10, 6.4 to 6.4.9 and 7.0 to 7.0.3 allows malicious webservers to retrieve a web proxy's client username and IP via same origin HTTP requests triggering proxy-generated HTTP status codes pages.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-231

Solution

See vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2021-43206
XREF	IAVA:2022-A-0221-S

Plugin Information

Published: 2022/05/27, Modified: 2023/05/24

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.10
```

197631 - Fortinet Fortigate (FG-IR-23-224)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-224 advisory.

- An exposure of sensitive information to an unauthorized actor in Fortinet FortiOS at least version at least 7.4.0 through 7.4.1 and 7.2.0 through 7.2.5 and 7.0.0 through 7.0.15 and 6.4.0 through 6.4.15 allows attacker to information disclosure via HTTP requests. (CVE-2024-23662)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-224

Solution

Upgrade to Fortigate version 7.2.6 / 7.4.2 or later.

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)

VPR Score

1.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-23662
XREF	IAVA:2024-A-0165

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

197623 - Fortinet Fortigate (FG-IR-23-225)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-225 advisory.

- An insufficient verification of data authenticity vulnerability [CWE-345] in Fortinet FortiOS SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.12 & FortiProxy SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.13 allows an authenticated VPN user to send (but not receive) packets spoofing the IP of another user via crafted network packets. (CVE-2023-45586)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-225

Solution

Upgrade to Fortigate version 7.0.13 / 7.2.8 / 7.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.0 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.6

EPSS Score

0.0004

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-45586
XREF	IAVA:2024-A-0165

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

197622 - Fortinet Fortigate (FG-IR-23-413)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-413 advisory.

- A use of externally-controlled format string vulnerability [CWE-134] in FortiOS version 7.4.1 and below, version 7.2.7 and below, 7.0 all versions, 6.4 all versions command line interface may allow a local privileged attacker with super-admin profile and CLI access to execute arbitrary code or commands via specially crafted requests. (CVE-2023-48784)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-413

Solution

Upgrade to Fortigate version 7.2.8 / 7.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-48784
XREF	IAVA:2024-A-0165

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

200327 - Fortinet Fortigate (FG-IR-23-423)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-423 advisory.

- A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file. (CVE-2024-21754)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-423

Solution

Upgrade to Fortigate version 7.0.999999 / 7.2.9 / 7.4.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

4.4 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

3.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.1

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-21754

Plugin Information

Published: 2024/06/11, Modified: 2024/10/07

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : See vendor advisory
```

190103 - Fortinet Fortigate (FG-IR-23-432)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-432 advisory.

- An improper access control vulnerability [CWE-284] in FortiOS version 7.2.0, version 7.0.13 and below, version 6.4.14 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below may allow a remote unauthenticated attacker to bypass the firewall deny geolocalisation policy via timing the bypass with a GeoIP database update. (CVE-2023-47536)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-432

Solution

Upgrade to Fortigate version 7.2.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-47536
XREF	IAVA:2024-A-0019-S

Plugin Information

Published: 2024/02/07, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

200355 - Fortinet Fortigate (FG-IR-23-471)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-471 advisory.

- A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file. (CVE-2024-23111)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-471

Solution

Upgrade to Fortigate version 6.4.999999 / 7.0.14 / 7.2.8 / 7.4.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

4.8 (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-23111

Plugin Information

Published: 2024/06/11, Modified: 2024/08/23

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : See vendor advisory
```

177264 - Fortinet Fortigate 's map server (FG-IR-22-468)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-468 advisory.

- An improper certificate validation vulnerability [CWE-295] in FortiOS 6.2 all versions, 6.4 all versions, 7.0.0 through 7.0.10, 7.2.0 and FortiProxy 1.2 all versions, 2.0 all versions, 7.0.0 through 7.0.9, 7.2.0 through 7.2.3 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the vulnerable device and the remote FortiGuard's map server.

(CVE-2023-29175)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-468

Solution

Please upgrade to FortiOS version 7.2.1 or above Please upgrade to FortiOS version 7.0.11 or above Please upgrade to FortiProxy version 7.2.4 or above Please upgrade to FortiProxy version 7.0.10 or above

Risk Factor

Medium

CVSS v3.0 Base Score

4.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.5

EPSS Score

0.0005

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-29175
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/13, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.11
```

172395 - Fortinet Fortigate - Access of NULL pointer in SSLVPNd (FG-IR-22-477)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-477 advisory.

- An access of uninitialized pointer vulnerability [CWE-824] in the SSL VPN portal of Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.11 and FortiProxy version 7.2.0 through 7.2.1, version 7.0.0 through 7.0.7 and before 2.0.11 allows a remote authenticated attacker to crash the sslvpn daemon via an HTTP GET request. (CVE-2022-45861)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-477

Solution

Upgrade to Fortigate version 6.4.12 / 7.0.10 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-45861
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2023/03/09, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

177124 - Fortinet Fortigate - Access of uninitialized pointer in administrative interface API (FG-IR-23-095)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-095 advisory.

- A access of uninitialized pointer vulnerability [CWE-824] in Fortinet FortiProxy version 7.2.0 through 7.2.3 and before 7.0.9 and FortiOS version 7.2.0 through 7.2.4 and before 7.0.11 allows an authenticated attacker to repetitively crash the httpsd process via crafted HTTP or HTTPS requests. (CVE-2023-29178)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-095

Solution

Please upgrade to FortiProxy version 7.2.4 or above Please upgrade to FortiProxy version 7.0.10 or above Please upgrade to FortiOS version 7.2.5 or above Please upgrade to FortiOS version 7.0.12 or above

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0005

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-29178
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.12
```

179503 - Fortinet Fortigate - Buffer overflow in execute extender command (FG-IR-23-149)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-149 advisory.

- A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiOS before 7.0.3 allows a privileged attacker to execute arbitrary code via specially crafted CLI commands, provided the attacker were able to evade FortiOS stack protections. (CVE-2023-29182)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-149

https://code610.blogspot.com/2023/04/fuzzing-fortigate-7.html

Solution

Please upgrade to FortiOS version 7.4.0 or above

Please upgrade to FortiOS version 7.2.0 or above

Please upgrade to FortiOS version 7.0.4 or above

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0006

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-29182
XREF	IAVA:2023-A-0353-S

Plugin Information

Published: 2023/08/08, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.4
```

185608 - Fortinet Fortigate - DOS in headers management (FG-IR-23-151)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-151 advisory.

- A numeric truncation error in Fortinet FortiProxy version 7.2.0 through 7.2.4, FortiProxy version 7.0.0 through 7.0.10, FortiProxy 2.0 all versions, FortiProxy 1.2 all versions, FortiProxy 1.1, all versions, FortiProxy 1.0 all versions, FortiOS version 7.4.0, FortiOS version 7.2.0 through 7.2.5, FortiOS version 7.0.0 through 7.0.12, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions allows attacker to denial of service via specifically crafted HTTP requests. (CVE-2023-36641)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-151

Solution

Upgrade to Fortigate version 7.0.13 / 7.2.6 / 7.4.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-36641
XREF	IAVA:2023-A-0643-S

Plugin Information

Published: 2023/11/14, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

177119 - Fortinet Fortigate - DoS in firmware upgrade function (FG-IR-22-375)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-375 advisory.

- A loop with unreachable exit condition ('infinite loop') in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS version 7.0.0 through 7.0.10, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions, FortiProxy version 7.2.0 through 7.2.3, FortiProxy version 7.0.0 through 7.0.9, FortiProxy 2.0 all versions, FortiProxy 1.2 all versions, FortiProxy 1.1 all versions, FortiProxy 1.0 all versions, FortiWeb version 7.2.0 through 7.2.1, FortiWeb version 7.0.0 through 7.0.6, FortiWeb 6.4 all versions, FortiWeb 6.3 all versions allows attacker to perform a denial of service via specially crafted HTTP requests. (CVE-2023-33305)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-375

Solution

Please upgrade to FortiPAM version 1.0.0 or above Please upgrade to FortiWeb version 7.2.2 or above Please upgrade to FortiWeb version 7.0.7 or above Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.5 or above Please upgrade to FortiOS version 7.0.11 or above Please upgrade to FortiProxy version 7.2.4 or above Please upgrade to FortiProxy version 7.0.10 or above

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-33305
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.11
```

177120 - Fortinet Fortigate - Null pointer dereference in sslvpnd proxy endpoint (FG-IR-23-125)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-125 advisory.

- A null pointer dereference in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, Fortiproxy version 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 allows attacker to denial of service via specially crafted HTTP requests. (CVE-2023-29179)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-125

Solution

Please upgrade to FortiOS version 7.4.0 or above

Please upgrade to FortiOS version 7.2.5 or above

Please upgrade to FortiOS version 7.0.12 or above

Please upgrade to FortiOS version 6.4.13 or above

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-29179
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

174237 - Fortinet Fortigate - Open redirect in sslvpnd (FG-IR-22-479)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-479 advisory.

- A url redirection to untrusted site ('open redirect') in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.9, FortiOS versions 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specially crafted requests. (CVE-2023-22641)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-479

Solution

Please upgrade to FortiProxy version 7.2.3 or above Please upgrade to FortiProxy version 7.0.9 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.10 or above Please upgrade to FortiOS version 6.4.13 or above

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0005

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-22641
XREF	IAVA:2023-A-0198-S

Plugin Information

Published: 2023/04/13, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

171888 - Fortinet Fortigate - Padding oracle in cookie encryption (FG-IR-21-126)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-21-126 advisory.

- An improper verification of cryptographic signature vulnerability [CWE-347] in FortiWeb 6.4 all versions, 6.3.16 and below, 6.2 all versions, 6.1 all versions, 6.0 all versions; FortiOS 7.0.3 and below, 6.4.8 and below, 6.2 all versions, 6.0 all versions; FortiSwitch 7.0.3 and below, 6.4.10 and below, 6.2 all versions, 6.0 all versions; FortiProxy 7.0.1 and below, 2.0.7 and below, 1.2 all versions, 1.1 all versions, 1.0 all versions may allow an attacker to decrypt portions of the administrative session management cookie if able to intercept the latter. (CVE-2021-43074)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-126

Solution

Upgrade to Fortigate version 6.4.9 / 7.0.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0005

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-43074
XREF	IAVA:2023-A-0110-S

Plugin Information

Published: 2023/02/24, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.9
```

177123 - Fortinet Fortigate - SMTP password ciphertext exposure in Log (FG-IR-22-455)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-455 advisory.

- An insertion of sensitive information into log file vulnerability [CWE-532] in FortiOS / FortiProxy log events may allow a remote authenticated attacker to read certain passwords in plain text. (CVE-2023-26207)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-455

Solution

Please upgrade to FortiOS version 7.2.6, 7.4.0 or above.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-26207
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2023/12/01

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.2.6 / 7.4.0
```

197609 - Fortinet Fortigate - Unauthenticated access to static files containing logging information (FG-IR-22-364)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-364 advisory.

- An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiOS version 7.2.0 through 7.2.3 and 7.0.0 through 7.0.9 allows an unauthenticated attackers to obtain sensitive logging informations on the device via crafted HTTP GET requests. (CVE-2022-41329)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-364

Solution

Upgrade to Fortigate version 6.4.12 / 7.0.10 / 7.2.4 or later.

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)

VPR Score

1.4

EPSS Score

0.0018

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-41329
XREF	IAVA:2023-A-0125-S

Plugin Information

Published: 2024/05/22, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

174402 - Fortinet Fortigate - header injection in proxy login page (FG-IR-22-362)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-362 advisory.

- A improper neutralization of crlf sequences in http headers ('http response splitting') in Fortinet FortiOS versions 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.11, 6.2.0 through 6.2.12, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.1, 7.0.0 through 7.0.7, 2.0.0 through 2.0.10, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6 may allow an authenticated and remote attacker to perform an HTTP request splitting attack which gives attackers control of the remaining headers and body of the response.

(CVE-2022-42472)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-362

Solution

Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above Please upgrade to FortiProxy version 2.0.11 or above Please upgrade to FortiOS version 7.2.3 or above Please upgrade to FortiOS version 7.0.9 or above Please upgrade to FortiOS version 6.4.13 or above

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.5

EPSS Score

0.0008

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-42472
XREF	IAVA:2023-A-0110-S

Plugin Information

Published: 2023/04/17, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

177387 - Fortinet Fortigate : authenticated user null pointer dereference in SSL-VPN (FG-IR-23-015)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-015 advisory.

- A null pointer dereference in Fortinet FortiOS before 7.2.5, before 7.0.11 and before 6.4.13, FortiProxy before 7.2.4 and before 7.0.10 allows attacker to denial of sslvpn service via specifically crafted request in bookmark parameter. (CVE-2023-33306)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-015

Solution

Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.5 or above Please upgrade to FortiOS version 7.0.11 or above Please upgrade to FortiOS version 6.4.13 or above Please upgrade to FortiProxy version 7.2.4 or above Please upgrade to FortiProxy version 7.0.10 or above

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-33306
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/16, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

185607 - Fortinet Fortigate VM - Bypass of root file system integrity checks at boot time on VM (FG-IR-22-396)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-396 advisory.

- An improper validation of integrity check value vulnerability [CWE-354] in FortiOS 7.2.0 through 7.2.3, 7.0.0 through 7.0.12, 6.4 all versions, 6.2 all versions, 6.0 all versions and FortiProxy 7.2 all versions, 7.0 all versions, 2.0 all versions VMs may allow a local attacker with admin privileges to boot a malicious image on the device and bypass the filesystem integrity check in place. (CVE-2023-28002)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-396

Solution

Upgrade to Fortigate version 7.0.13 / 7.2.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.5 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-28002
XREF	IAVA:2023-A-0643-S

Plugin Information

Published: 2023/11/14, Modified: 2024/05/28

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : Migrate to a fixed release.
```

165179 - Fortinet Fortigate xss (FG-IR-21-222)

Synopsis

The remote host is affected by a xss vulnerability.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-21-222 advisory.

- An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiOS may allow an authenticated attacker to perform a stored cross site scripting (XSS) attack through the URI parameter via the Threat Feed IP address section of the Security Fabric External connectors. (CVE-2021-43080)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Fortigate version 6.4.10 / 7.0.6 / 7.2.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0005

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-43080
XREF	IAVA:2022-A-0357-S

Plugin Information

Published: 2022/09/15, Modified: 2022/12/05

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.10
```

179480 - Fortinet Fortigate xss (FG-IR-21-248)

Synopsis

Remote host is affected by a xss vulnerability.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-21-248 advisory.

- A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiOS 6.0.7 - 6.0.15, 6.2.2 - 6.2.12, 6.4.0 - 6.4.9 and 7.0.0 - 7.0.3 allows a privileged attacker to execute unauthorized code or commands via storing malicious payloads in replacement messages. (CVE-2022-40680)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-21-248

Solution

Please upgrade to FortiOS version 7.2.2 Please upgrade to FortiOS version 7.0.7 Please upgrade to FortiOS version 6.4.10 or above

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0005

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2022-40680
XREF	IAVA:2022-A-0458-S

Plugin Information

Published: 2023/08/08, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.10
```

174264 - Fortinet Fortigate xss (FG-IR-22-363)

Synopsis

Remote host is affected by a xss vulnerability.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-363 advisory.

- An improper neutralization of input during web page generation vulnerability ('Cross-site Scripting') [CWE-79] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9, version 6.4.0 through 6.4.11 and before 6.2.12 and FortiProxy version 7.2.0 through 7.2.1 and before 7.0.7 allows an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests. (CVE-2022-41330)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-363

Solution

Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.10 or above Please upgrade to FortiOS version 6.4.12 or above Please upgrade to FortiOS version 6.2.13 or above

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-41330
XREF	IAVA:2023-A-0198-S

Plugin Information

Published: 2023/04/13, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.12
```

181358 - Fortinet Fortigate xss (FG-IR-23-106)

Synopsis

Remote host is affected by a xss vulnerability.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-23-106 advisory.

- An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiProxy 7.2.0 through 7.2.4, 7.0.0 through 7.0.10 and FortiOS 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.14 GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management setting. (CVE-2023-29183)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-23-106

Solution

Please upgrade to FortiProxy version 7.2.5 or above Please upgrade to FortiProxy version 7.0.11 or above Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.5 or above Please upgrade to FortiOS version 7.0.12 or above Please upgrade to FortiOS version 6.4.13 or above Please upgrade to FortiOS version 6.2.15 or above

Risk Factor

Medium

CVSS v3.0 Base Score

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.0

EPSS Score

0.0006

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-29183
XREF	IAVA:2023-A-0486

Plugin Information

Published: 2023/09/13, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.1

EPSS Score

0.9654

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following CBC Client to Server algorithm               : aes256-cbc
Supports following CBC Client to Server algorithm               : rijndael-cbc@lysator.liu.se
Supports following CBC Client to Server algorithm               : aes192-cbc
Supports following CBC Client to Server algorithm               : cast128-cbc
Supports following CBC Client to Server algorithm               : blowfish-cbc
Supports following CBC Client to Server algorithm               : 3des-cbc
Supports following CBC Client to Server algorithm               : aes128-cbc
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-ripemd160-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following CBC Server to Client algorithm               : aes256-cbc
Supports following CBC Server to Client algorithm               : rijndael-cbc@lysator.liu.se
Supports following CBC Server to Client algorithm               : aes192-cbc
Supports following CBC Server to Client algorithm               : cast128-cbc
Supports following CBC Server to Client algorithm               : blowfish-cbc
Supports following CBC Server to Client algorithm               : 3des-cbc
Supports following CBC Server to Client algorithm               : aes128- [...]
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

174401 - Fortinet Fortigate - Flaws over DHCP and DNS keys encryption scheme (FG-IR-22-080)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-080 advisory.

- A missing cryptographic steps vulnerability [CWE-325] in the functions that encrypt the DHCP and DNS keys in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.9, 6.2.x and 6.0.x may allow an attacker in possession of the encrypted key to decipher it. (CVE-2022-29054)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-080

Solution

Please upgrade to FortiOS version 7.2.1 or above Please upgrade to FortiOS version 7.0.8 or above Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0004

CVSS v2.0 Base Score

1.7 (CVSS2#AV:L/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-29054
XREF	IAVA:2023-A-0110-S

Plugin Information

Published: 2023/04/17, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.8
```

165242 - Fortinet Fortigate - Flaws over krb keytab encryption scheme (FG-IR-22-158)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-158 advisory.

- A missing cryptographic steps vulnerability [CWE-325]in the functions that encrypt the keytab files in FortiOS may allow anattacker in possession of the encrypted file to decipher it. (CVE-2022-29053)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Fortigate version 7.0.6 / 7.2.1 or later.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0004

CVSS v2.0 Base Score

1.7 (CVSS2#AV:L/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2022-29053

Plugin Information

Published: 2022/09/19, Modified: 2022/12/02

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 7.0.6
```

177121 - Fortinet Fortigate - Path traversal vulnerability in administrative interface (FG-IR-22-393)

Synopsis

Fortinet Firewall is missing one or more security-related updates.

Description

The version of Fortigate installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the FG-IR-22-393 advisory.

- A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.12, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiSwitchManager version 7.2.0 through 7.2.1 and before 7.0.1 allows an privileged attacker to delete arbitrary directories from the filesystem through crafted HTTP requests. (CVE-2022-42474)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.fortiguard.com/psirt/FG-IR-22-393

Solution

Please upgrade to FortiOS version 7.4.0 or above Please upgrade to FortiOS version 7.2.4 or above Please upgrade to FortiOS version 7.0.10 or above Please upgrade to FortiOS version 6.4.13 or above Please upgrade to FortiSwitchManager version 7.2.2 or above Please upgrade to FortiSwitchManager version 7.0.2 or above Please upgrade to FortiProxy version 7.2.2 or above Please upgrade to FortiProxy version 7.0.8 or above Please upgrade to FortiProxy version 2.0.12 or above

Risk Factor

Low

CVSS v3.0 Base Score

2.7 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

2.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.2

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-42474
XREF	IAVA:2023-A-0281-S

Plugin Information

Published: 2023/06/12, Modified: 2024/05/22

Plugin Output

tcp/0

```
Installed version : 6.4.5
Fixed version     : 6.4.13
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

4.2

EPSS Score

0.8808

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

VPR Score

3.6

EPSS Score

0.5961

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

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

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/10/10

Plugin Output

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:fortinet:fortios -> Fortinet FortiOS
  cpe:/o:fortinet:fortios:%3e%3d_5.4 -> Fortinet FortiOS
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : firewall
Confidence level : 100
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:EF:42:28 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:EF:42:28
```

73522 - Fortinet Device Detection

Synopsis

It was possible to obtain the operating system version number of the remote Fortinet device.

Description

The remote host is a Fortinet device. It was possible to read the OS version number by logging into the device via SSH.

See Also

https://www.fortinet.com/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0603

Plugin Information

Published: 2014/04/15, Modified: 2024/10/10

Plugin Output

tcp/0

```
Model   : FortiGate-VM64
Version : 6.4.5
Build   : 1828
SN      : FGVMEVAEYM0CHXA7
Uptime : 0 days,  0 hours,  15 minutes
```

17367 - Fortinet FortiGate Web Console Management Detection

Synopsis

A firewall management console is running on the remote host.

Description

A Fortinet FortiGate Firewall is running on the remote host, and connections are allowed to its web-based console management port.

Letting attackers know that you are using this software will help them to focus their attack or will make them change their strategy. In addition to this, an attacker may set up a brute-force attack against the remote interface.

See Also

https://www.fortinet.com/products/fortigate/

Solution

Filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2005/03/18, Modified: 2023/07/18

Plugin Output

tcp/80/www

```
The following instance of FortiOS Web Interface was detected on the remote host :

  Version : >= 5.4
  URL     : http://192.168.217.100/
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sat, 19 Oct 2024 20:16:01 GMT
  Location: http://192.168.217.100/ng
  Content-Length: 209
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://192.168.217.100/ng">here</a>.</p>
</body></html>
```

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 is 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: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sat, 19 Oct 2024 20:16:01 GMT
  Location: http://192.168.217.100:443/ng
  Content-Length: 213
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://192.168.217.100:443/ng">here</a>.</p>
</body></html>
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2024/03/13

Plugin Output

tcp/0

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: 2024/05/20

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/443/www

```
Port 443/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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202410161649
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : FortiGate 6.4.5 - 192.168.217.100
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.217.1
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 96.364 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'admin' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 50
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/10/19 23:12 Egypt Standard Time
Scan duration : 846 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : FortiOS on Fortinet FortiGate
Confidence level : 100
Method : HTML


The remote host is running FortiOS on Fortinet FortiGate
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2024/10/15

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

Local checks have been enabled for this host.
The remote FortiOS system is:
Version: 6.4.5,build1828,210217
  Model: FortiGate-VM64

OS Security Patch Assessment is available for this host.
Runtime : 258.816790 seconds
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account  : admin
Protocol : SSH
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/10/15

Plugin Output

tcp/0

```
. You need to take the following 4 actions :

[ Fortinet FortiOS - Information Disclosure (FG-IR-22-364) (172492) ]

+ Action to take : Upgrade to Fortigate version 6.4.12 / 7.0.10 / 7.2.4 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Fortinet FortiOS - Path Traversal Vulnerability (FG-IR-22-401) (172579) ]

+ Action to take : Upgrade to Fortigate version 6.2.13 / 6.4.12 / 7.0.9 / 7.2.4 or later.


[ Fortinet Fortigate - SMTP password ciphertext exposure in Log (FG-IR-22-455) (177123) ]

+ Action to take : Please upgrade to FortiOS version 7.2.6, 7.4.0 or above.


[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or
 disable the affected algorithms.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
```

```
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

Th [...]
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-p5O9b
SSH supported authentication : publickey,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       'admin'
Port:       22
Proto:      SSH
Method:     password
Escalation: Nothing
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User:       'admin'
Port:       22
Proto:      SSH
Method:     password
Escalation: Nothing
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.217.1 to 192.168.217.100 :
192.168.217.1
192.168.217.100

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : EDIT_HISTORY_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : ccsrftoken_10657207059885796103
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : VDOM_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : FILE_DOWNLOADING_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : APSCOOKIE_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_10657207059885796103
```

```
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : session_key_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies are expired :

Name : EDIT_HISTORY_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : ccsrftoken_10657207059885796103
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : VDOM_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : FILE_DOWNLOADING_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : APSCOOKIE_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_10657207059885796103
```

```
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : session_key_10657207059885796103
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Fri, 01-Nov-1974 20:15:32 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```