NETFORMERS

Testy Podatności - Raport

Warszawa, 28 listopad 2017

Spis treści

Podsumowanie

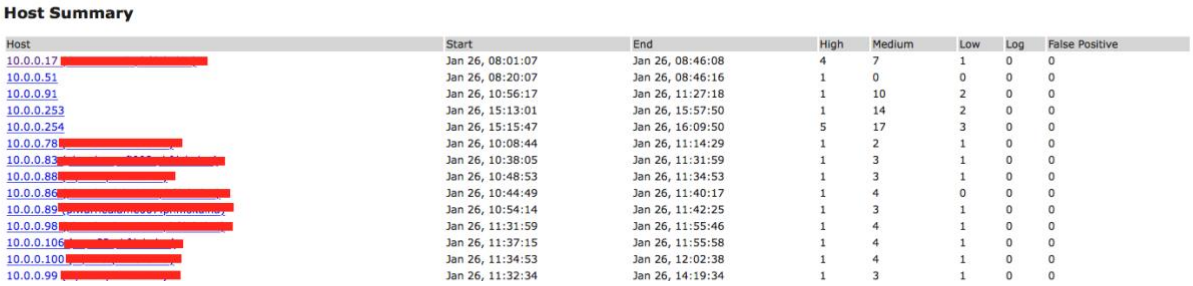
Niniejszy dokument jest podsumowaniem badania podatności wykonanego specjalistycznym skanerem podatności. W pierwszej części przedstawiono ogólny rezultat testów, natomiast w drugiej części szczegółowo opisano podatności systemów. Dokument służy do celów poglądowych zawiera jednak wyniki testów rzeczywistego środowiska.

Podczas testów penetracyjnych wykonywano skrypty które mogłyby być wykorzystane podczas wykonywania cyber-ataków na stacjach końcowych oraz serwerach. Znalezione typy podatności mogą być wykorzystane m.in. do:

- Uzyskania danych użytkowników (np. loginy i hasła), danych przetwarzanych przez system (np. dane osobowe, listy przedsiębiorców)
- Dalszych ataków na inne hosty znajdujących się w sieci lokalnej
- Wykonywania złośliwego typu oprogramowania (np. Ransomware – zaszyfrowanie wszystkich plików na dyskach i zasobach sieciowych)

Rozpoczęcie skanu: **Fri Jan 26 08:00:34 2018 CET**

Zakończenie skanu: Fri Jan 26 18:27:54 2018 CET



Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
10.0.0.17 [redacted]	Jan 26, 08:01:07	Jan 26, 08:46:08	4	7	1	0	0
10.0.0.51	Jan 26, 08:20:07	Jan 26, 08:46:16	1	0	0	0	0
10.0.0.91	Jan 26, 10:56:17	Jan 26, 11:27:18	1	10	2	0	0
10.0.0.253	Jan 26, 15:13:01	Jan 26, 15:57:50	1	14	2	0	0
10.0.0.254	Jan 26, 15:15:47	Jan 26, 16:09:50	5	17	3	0	0
10.0.0.78 [redacted]	Jan 26, 10:08:44	Jan 26, 11:14:29	1	2	1	0	0
10.0.0.83 [redacted]	Jan 26, 10:38:05	Jan 26, 11:31:59	1	3	1	0	0
10.0.0.88 [redacted]	Jan 26, 10:48:53	Jan 26, 11:34:53	1	3	1	0	0
10.0.0.86 [redacted]	Jan 26, 10:44:49	Jan 26, 11:40:17	1	4	0	0	0
10.0.0.89 [redacted]	Jan 26, 10:54:14	Jan 26, 11:42:25	1	3	1	0	0
10.0.0.98 [redacted]	Jan 26, 11:31:59	Jan 26, 11:55:46	1	4	1	0	0
10.0.0.106 [redacted]	Jan 26, 11:37:15	Jan 26, 11:55:58	1	4	1	0	0
10.0.0.100 [redacted]	Jan 26, 11:34:53	Jan 26, 12:02:38	1	4	1	0	0
10.0.0.99 [redacted]	Jan 26, 11:32:34	Jan 26, 14:19:34	1	3	1	0	0

Rys1. Podsumowanie – podatności

W wynikach raportu szczegółowo zostały opisane podatności. Wykrywane podatności zawierają informacje tj.:

- nazwę podatności (wskazującą na rodzaj zagrożenia)
- nr wersji oprogramowania hosta
- ogólny opis podatności
- rezultat wykonanego skryptu podatności oraz opis używanej metody wykrywania podatności
- opis rozwiązania problemu
- wpływ na działanie systemu
- referencje.

Host 10.0.0.91

Scanning of this host started at: Fri Jan 26 10:56:17 2018 CET

Number of results: 13

Port Summary for Host 10.0.0.91

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

Security Issues for Host 10.0.0.91

general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Product detection result: cpe:/o:debian:debian_linux:6.0 by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Summary

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should

not be used anymore

Opis podatności – brak wsparcia dla oprogramowania, OS EoL

Vulnerability Detection Result

```
The "Debian GNU/Linux" Operating System on the remote host has reached the
end of life.

CPE:                 cpe:/o:debian:debian_linux:6.0
Installed version,
build or SP:         6.0
EOL date:            2016-02-29
EOL info:
https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table
```

Vulnerability Detection Method

Details: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Version used: $Revision: 7864 $

Product Detection Result

Product: cpe:/o:debian:debian_linux:6.0

Method: OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Summary

The remote server's SSL/TLS certificate has already expired.

Opis podatności – wygaśnięcie certyfikatu

Vulnerability Detection Result

```
The certificate of the remote service expired on 2015-03-11 19:54:33.

Certificate details:
subject ...: CN=10.0.0.94,OU=Nagios,O=xxxx,L=Warszawa,ST=Mazowieckie,C=PL
subject alternative names (SAN):
None
issued by .: CN=10.0.0.94,OU=Nagios,O=xxxx,L=Warszawa,ST=Mazowieckie,C=PL
serial ....: 00CD7191B0C9414CB3
valid from : 2014-03-11 19:54:33 UTC
valid until: 2015-03-11 19:54:33 UTC
fingerprint (SHA-1): 9BB0D38FE13261BA5D1E99EFE500CEDE10A3C26C
fingerprint (SHA-256):
34D751A3517BD50565510F10877710BE989B89F57B05EE1E7EC1EF3CBE317FDD
```

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Rozwiązanie - zamiana certyfikatu na nowy

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: $Revision: 7248 $

Host 10.0.0.78

Scanning of this host started at:	Fri Jan 26 10:08:44 2018 CET
Number of results:	4

Port Summary for Host 10.0.0.78

Service (Port)	Threat Level
3389/tcp	Medium
445/tcp	High
general/tcp	Low

Security Issues for Host 10.0.0.78

445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Summary

This host is missing a critical security update according to Microsoft Bulletin **MS17-010.**

Opis podatności – Podatność Micros oftu MS17-010

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to gain the ability to execute code on

the target server, also could lead to information disclosure from the server.

Impact Level: System

Wpływ na działanie systemu – możliwość wykonania złośliwego kodu na serwerze docelowym

Solution

Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned

hotfixes in the advisory from the below link,

https://technet.microsoft.com/library/security/MS17-010

Rozwiązanie problemu – aktualizacja oprogramowania, link z referencją

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft
Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft
Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft
Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft
Windows Server 2008 x32/x64 Edition Service Pack 2

Lista podatnych systemów

Vulnerability Insight

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method

Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Version used: $Revision: 7543 $

References

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, VE-2017-0147, CVE-2017-0148

BID: 96703, 96704, 96705, 96707, 96709, 96706

CERT: CB-K17/0435, DFN-CERT-2017-0448

Other: https://support.microsoft.com/en-in/kb/4013078
https://technet.microsoft.com/library/security/MS17-010
https://github.com/rapid7/metasploit-framework/pull/8167/files

Referencje

3389/tcp

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Summary

The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.

Opis podatności – słaby algorytm szyfrowania

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using
insecure signature algorithms:

Subject:              CN=host.test.lokalna
Signature Algorithm:  sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Rozwiązanie – Zmiana szyfrowania na SHA2

Vulnerability Insight

Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

Vulnerability Detection Method

Check which algorithm was used to sign the remote SSL/TLS Certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: $Revision: 4781 $

References

Other: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Host 10.0.0.56

Scanning of this host started at: Fri Jan 26 08:29:23 2018 CET

Number of results: 11

Port Summary for Host 10.0.0.56

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

Security Issues for Host 10.0.0.56

443/tcp

High (CVSS: 9.0)

NVT: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Summary

It was possible to login into the remote Web Application using default credentials.
As the NVT 'HTTP Brute Force Logins with default Credentials'
(OID: 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting
of this vulnerability takes place in this NVT instead. The script preference
'Report timeout' allows you to configure if such an timeout is reported.

Opis podatności – zalogowanie się do urządzenia z wykorzystaniem standardowego loginu i hasła

Vulnerability Detection Result

It was possible to login with the following credentials <Url>:<User>:<Password>:<HTTP status code>

https://10.0.0.56/:admin:admin:HTTP/1.1 200 Ok
https://10.0.0.56/:user:user:HTTP/1.1 200 Ok

Solution

Solution type: Mitigation

Change the password as soon as possible.

Rozwiązanie – zmiana hasła

Vulnerability Detection Method

Try to login with a number of known default credentials via HTTP Basic Auth.

Details: HTTP Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103240)

Version used: $Revision: 6680 $

Host 10.0.0.51

Scanning of this host started at:	Fri Jan 26 08:20:07 2018 CET
Number of results:	1

Port Summary for Host 10.0.0.51

Service (Port)	Threat Level
80/tcp	High

Security Issues for Host 10.0.0.51

80/tcp

High (CVSS: 10.0)
NVT: NETGEAR ProSAFE GS108T Default Password (OID: 1.3.6.1.4.1.25623.1.0.108309)

Summary

The remote NETGEAR ProSAFE GS108E device has the default password 'password'.

Opis podatności – wykorzystanie standardowego hasła

Vulnerability Detection Result
It was possible to login with the default password 'password'

Solution

Solution type: Workaround

Change the password.

Rozwiązanie – zmiana hasła

Affected Software/OS

NETGEAR ProSAFE GS108E devices. Other models might be also affected.

Vulnerability Detection Method

Details: NETGEAR ProSAFE GS108T Default Password (OID: 1.3.6.1.4.1.25623.1.0.108309)

Version used: $Revision: 8025 $

References
Other: https://www.netgear.com/support/product/GS108Ev3.aspx

Host 10.0.0.254

Scanning of this host started at: Fri Jan 26 15:15:47 2018 CET

Number of results: 25

Port Summary for Host 10.0.0.254

Service (Port)	Threat Level
443/tcp	Medium
general/tcp	High
5989/tcp	Medium

Security Issues for Host 10.0.0.254

general/tcp

High (CVSS: 10.0)
NVT: VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105394)

Summary

VMware vCenter and ESXi updates address critical security issues.

Opis podatności – możliwość wykonania zdalnego kodu

Vulnerability Detection Result
ESXi Version: 5.0.0
Detected Build: 469512
Fixed Build: 3021432
Solution

Rozwiązanie – wgranie patch'a; Lista podatnych systemów

Solution type: VendorFix

Apply the missing patch(es).

Affected Software/OS

VMware ESXi 5.5 without patch ESXi550-201509101 VMware ESXi 5.1 without patch ESXi510-201510101 VMware ESXi 5.0 without patch ESXi500-201510101

VMware vCenter Server 6.0 prior to version 6.0 update 1 VMware vCenter Server 5.5 prior to version 5.5 update 3 VMware vCenter Server 5.1 prior to version 5.1 update u3b VMware vCenter Server 5.0 prior to version 5.u update u3e

Vulnerability Insight

VMware ESXi OpenSLP Remote Code Execution VMware ESXi contains a double free flaw in OpenSLP's SLPDProcessMessage() function. Exploitation of this issue may allow an unauthenticated attacker to execute code remotely on the ESXi host.

VMware vCenter Server JMX RMI Remote Code Execution VMware vCenter Server contains a remotely accessible JMX RMI service that is not securely configured. An unauthenticated remote attacker that is able to connect to the service may be able use it to execute arbitrary code on the vCenter server.

VMware vCenter Server vpxd denial-of-service vulnerability VMware vCenter Server does not properly sanitize long heartbeat messages. Exploitation of this issue may allow an unauthenticated attacker to create a denial-of-service condition in the vpxd service.

Vulnerability Detection Method

Check the build number

Details: VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105394)

Version used: $Revision: 6497 $

References

CVE:	CVE-2015-5177, CVE-2015-2342, CVE-2015-1047
CERT:	CB-K15/1443, CB-K15/1304, DFN-CERT-2015-1519, DFN-CERT-2015-1368
Other:	http://www.vmware.com/security/advisories/VMSA-2015-0007.html

Medium (CVSS: 6.8)
NVT: HP Integrated Lights-Out XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.106481)

Product detection result: cpe:/o:hp:integrated_lights-out:1.40 by HP Integrated Lights-Out Detection (OID: 1.3.6.1.4.1.25623.1.0.20285)

Summary

HP Integrated Lights-Out is prone to a cross-site scripting vulnerability.

Opis podatności – podatność na atak typu XSS

Vulnerability Detection Result
Installed version: 1.40
Fixed version: 2.44
Solution

Solution type: VendorFix

Upgrade to firmware 1.88 (iLO 3), 2.44 (iLO 4)

Rozwiązanie problemu – aktualizacja oprogramowania

Affected Software/OS

HPE Integrated Lights-Out 3 (iLO 3) and HPE Integrated Lights-Out 4 (iLO 4)

Vulnerability Detection Method

Checks the version.

Details: HP Integrated Lights-Out XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.106481)

Version used: $Revision: 4800 $

Product Detection Result

Product:	cpe:/o:hp:integrated_lights-out:1.40
Method:	HP Integrated Lights-Out Detection (OID: 1.3.6.1.4.1.25623.1.0.20285)

References

CVE:	CVE-2016-4406
Other:	https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05337025