jamk.fi

Data security testing

Lab 2: Vulnerability scan

Timo Lehosvuo, M3426@student.jamk.fi

Raportti
Data Security Testing, Markku Vajaranta
Syksy 2020
Tieto- ja viestintätekniikan koulutusohjelma
Tekniikan ja liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisällysluettelo

1 Vulnerabilities in software 2

1.1 Tehtävä 1 2

2 Vulnerability scan 5

2.1 Topologia 5

2.2 Tehtävä 2 5

3 Vulnerability analysis 9

3.1 Haavoittuvuus 1 9

3.2 Haavoittuvuus 2 10

3.3 Haavoittuvuus 3 11

1 Vulnerabilities in software

1.1 Tehtävä 1

Vulnerabilities

- https://www.cvedetails.com/vulnerabilities-by-types.php

1. Use searches (or browse vulnerabilities) to look recent vulns.
2. Select one software from your computer

   Use search to find vulnerabilities related to the software/vendor

Kuva 1: Tehtävänanto 1.

Valitsin ohjelmaksi Firefox-selaimen mistä aloin etsimään haavoittuvuuksia. Käytin lähteenä sivustoa https://secinfo.greenbone.net/nvts mistä etsin uusimpia haavoittuvuuksia. Päätin tutkia kahta haavoittuvuutta eri käyttöjärjestelmille ja eri CVSS pisteillä. Tuorein haavoittuvuus oli löydetty viikko sitten (23.10.2020), joka koski päivittämätöntä ”firefox-esr” pakettia.

Debian: Security Advisory for firefox-esr (DSA-4778-1)	Debian Local Security Checks	Fri, Oct 23, 2020 3:00 AM UTC	Tue, Oct 27, 2020 8:31 AM UTC	CVE-2020-15683 CVE-2020-15969		5.0 (Medium)	97 %

Kuva 2: Haavoittuvuus 1.

Haavoittuvuuden CVSS pisteet oli 5.0 ja se koski Firefox-selainta Linux Debian käyttöjärjestelmässä. Haavoittuvuus ei ole vakavuudella kovin hälyttävä sillä 5 CVSS pistettä (medium) ei ole vielä kovin hälyttävä. Tämä haavoittuvuus mahdollisti koodin ajamisen sovelluksessa. Haavoittuvuuden korjaaminen on hyvin yksinkertaista, sillä ei tarvitse kuin päivittää paketti tai koko sovellus.

Debian: Security Advisory for firefox-esr (DSA-4778-1)	Debian Local Security Checks	Fri, Oct 23, 2020 3:00 AM UTC	Tue, Oct 27, 2020 8:31 AM UTC	CVE-2020-15683 CVE-2020-15969	5.0 (Medium)	97 %

Summary

The remote host is missing an update for the 'firefox-esr' package(s) announced via the DSA-4778-1 advisory.

Scoring

CVSS Base 5.0 (Medium)

CVSS Base Vector AV:N/AC:L/Au:N/C:P/I:N/A:N

Insight

Multiple security issues have been found in the Mozilla Firefox web browser, which could potentially result in the execution of arbitrary code.

Detection Method

Checks if a vulnerable package version is present on the target host.
Quality of Detection: package (97%)

Affected Software/OS

'firefox-esr' package(s) on Debian Linux.

Solution

Solution Type: Vendorfix
For the stable distribution (buster), these problems have been fixed in version 78.4.0esr-1~deb10u2.

We recommend that you upgrade your firefox-esr packages.

Kuva 3: Haavoittuvuus 1.1.

Toiseksi haavoittuvuudeksi valitsin haavoittuvuuden Windows-käyttöjärjestelmälle, sillä käytän sitä itse pääsääntöisesti. Haavoittuvuus oli löydetty 21.10.2020 ja se oli CVSS arvoltaan 10 (high).

Mozilla Firefox Security Updates(mfsa_2020-45_2020-46)-Windows	General	Wed, Oct 21, 2020 4:51 AM UTC	Tue, Oct 27, 2020 8:31 AM UTC	CVE-2020-15969 CVE-2020-15254 CVE-2020-15680 CVE-2020-15681 CVE-2020-15682 CVE-2020-15683 CVE-2020-15684	10.0 (High)	97 %

Kuva 4: Haavoittuvuus 2.

CVSS pisteistä voidaan päätellä, että kyseessä on hyvin vakava haavoittuvuus, joka on parasta korjata mahdollisimman nopeasti. Raportti pitää sisällään useamman haavoittuvuuden, tosin kaikki näistä haavoittuvuuksista eivät ole vakavia.

Insight

Multiple flaws exist due to:

- Use-after-free in usersctp.

- Undefined behavior in bounded channel of crossbeam rust crate.

- Presence of external protocol handlers could be determined through image tags.

- Multiple WASM threads may have overwritten each others&#39, stub table entries.

- The domain associated with the prompt to open an external protocol could be spoofed to display the incorrect origin.

- Memory safety bugs fixed in Firefox 82 and Firefox ESR 78.4.

- Memory safety bugs fixed in Firefox 82.

Kuva 5: Haavoittuvuus 2.1.

Nämä haavoittuvuudet ovat korjattu Firefox-selaimen versiossa 82 ja ovat läsnä vain aikaisemmissa versioissa. Osa haavoittuvuuksista mahdollistavat koodin ajamisen sovelluksessa ja mahdollisen DoS-hyökkäyksen. Haavoittuvuuden korjaaminen tapahtuu siis päivittämällä selaimen versio versioon 82 tai uudempaan

Summary

This host is installed with
Mozilla Firefox and is prone to multiple vulnerabilities.

Scoring

CVSS Base 10.0 (High)

CVSS Base Vector AV:N/AC:L/Au:N/C:C/I:C/A:C

Insight

Multiple flaws exist due to:

- Use-after-free in usersctp.

- Undefined behavior in bounded channel of crossbeam rust crate.

- Presence of external protocol handlers could be determined through image tags.

- Multiple WASM threads may have overwritten each others&#39, stub table entries.

- The domain associated with the prompt to open an external protocol could be spoofed to display the incorrect origin.

- Memory safety bugs fixed in Firefox 82 and Firefox ESR 78.4.

- Memory safety bugs fixed in Firefox 82.

Detection Method

Checks if a vulnerable version is present on the target host.
Quality of Detection: registry (97%)

Affected Software/OS

Mozilla Firefox version before
82 on Windows.

Impact

Successful exploitation will allow
attackers to conduct a denial-of-service or execute arbitrary code
on affected system.

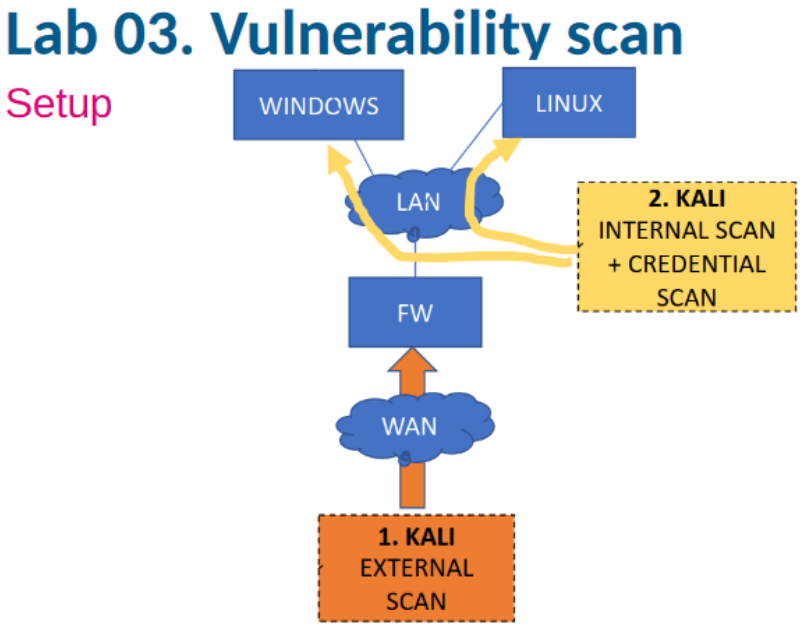
Solution

Solution Type: Vendorfix
Upgrade to Mozilla Firefox version 82
or later, Please see the references for more information.

Kuva 6: Haavoittuvuus 2.2.

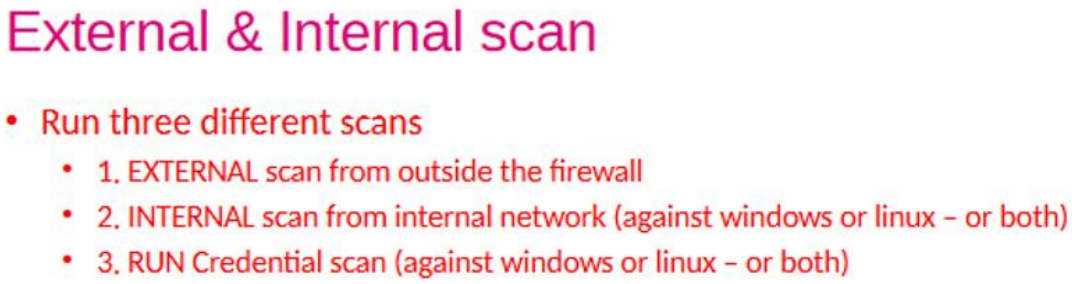
2 Vulnerability scan

2.1 Topologia



Kuva 7: Topologia.

2.2 Tehtävä 2



Kuva 8: Tehtävänanto 2.

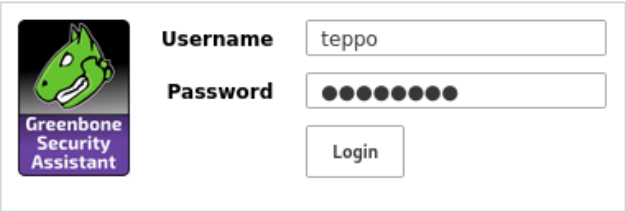
Aloitin tehtävän tekemisen käynnistämällä tarvittavat virtuaalikoneet: Kali, Linux, Firewall ja windows 7. Seuraavaksi käynnistin OpenVAS:in komennolla ”sudo gvm-start”:

```
sudouser@kali:~$ sudo gvm-start
[sudo] password for sudouser:
[*] Please wait for the GVM / OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
     Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; d
isabled; vendor preset: disabled)
     Active: active (running) since Thu 2020-10-29 14:28:33 EDT; 5s ago
       Docs: man:gsad(8)
             https://www.greenbone.net
```

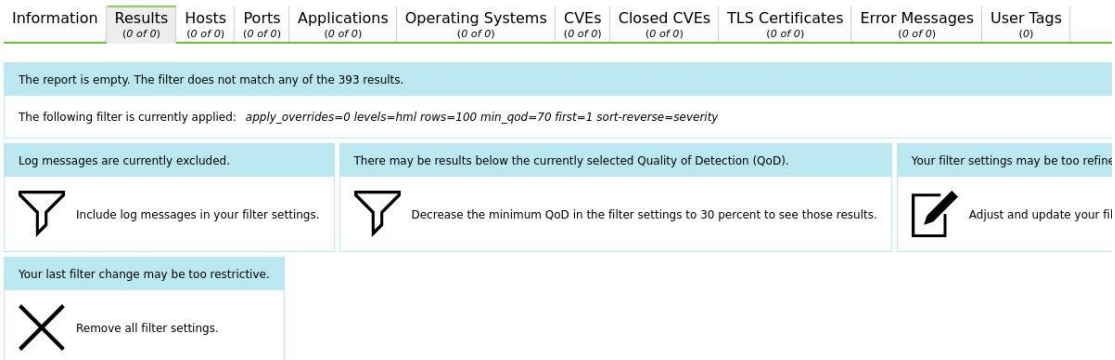
Kuva 9: OpenVAS käynnistys.

Tämän jälkeen kirjauduin sisään (osoite 127.0.0.1:9392).



Kuva 10: OpenVAS kirjautuminen.

ja aloitin tehtävän skannaamalla palomuuria ulkoverkosta käsin.



Kuva 11: Palomuurin skannaus.

Kuten kuvasta näkyy skannaus ei anna minkäänlaista tulosta, joka kertoo oikein konfiguroidusta palomuurista.

✖	Oct 15 10:06:36	WAN	Default deny rule IPv4 (1000000103)	192.168.43.98	192.168.43.72	ICMP
✖	Oct 15 10:06:37	WAN	Default deny rule IPv4 (1000000103)	192.168.43.98	192.168.43.72	ICMP

Kuva 12: Ping deny

Tutkin vielä palomuurin lokitietoja lisää ja löysin estetyn ping-pyynnön.

Jatkoin tehtävän tekemistä skannaamalla Linuxia verkon sisältäpäin

Information | Results (5 of 133) | Hosts (1 of 1) | Ports (2 of 2) | Applications (3 of 3) | Operating Systems (1 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 5 of 5

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Source Control Management (SCM) Files Accessible		5.0 (Medium)	80 %	10.99.67.145		80/tcp	Thu, Oct 15, 2020 8:51 AM UTC
Missing `httpOnly` Cookie Attribute		5.0 (Medium)	80 %	10.99.67.145		80/tcp	Thu, Oct 15, 2020 8:51 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	10.99.67.145		80/tcp	Thu, Oct 15, 2020 8:51 AM UTC
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95 %	10.99.67.145		22/tcp	Thu, Oct 15, 2020 8:50 AM UTC
TCP timestamps		2.6 (Low)	80 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 8:50 AM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

Kuva 13: Linux scan

Kuten huomataan sisäverkosta tehty skannaus antaa jo tuloksia. Löydetyt haavoittuvuuden ovat CVSS arvoltaan 5 tai alle. Tämä kertoo, että löydetyt haavoittuvuudet eivät ole kovin vakavia, tosin niitä on 133 kappaletta. Jatkoin Linuxin skannailua mutta tällä kertaa tein ”credentiaali” skannauksen. Ensiksi tein ”credential” tiedoston, joka sisälsi Linuxin käyttäjänimen ja salasanan.

Name ▲	Type	Allow insecure use	Login	Actions
Linux credential (centos root)	Username + Password (up)	No	root	

Comment	centos root
Type	Username + Password (up)
Allow Insecure Use	No
Login	root

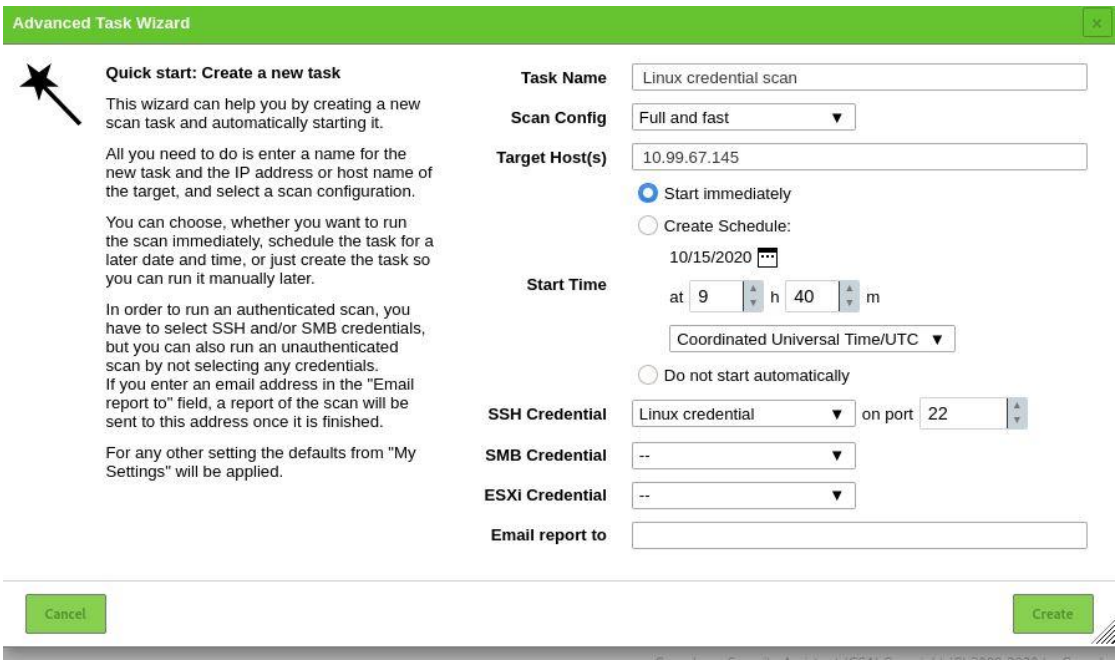
Apply to page contents

(Applied filter: sort=name first=1 rows=10)

1 - 1 of 1

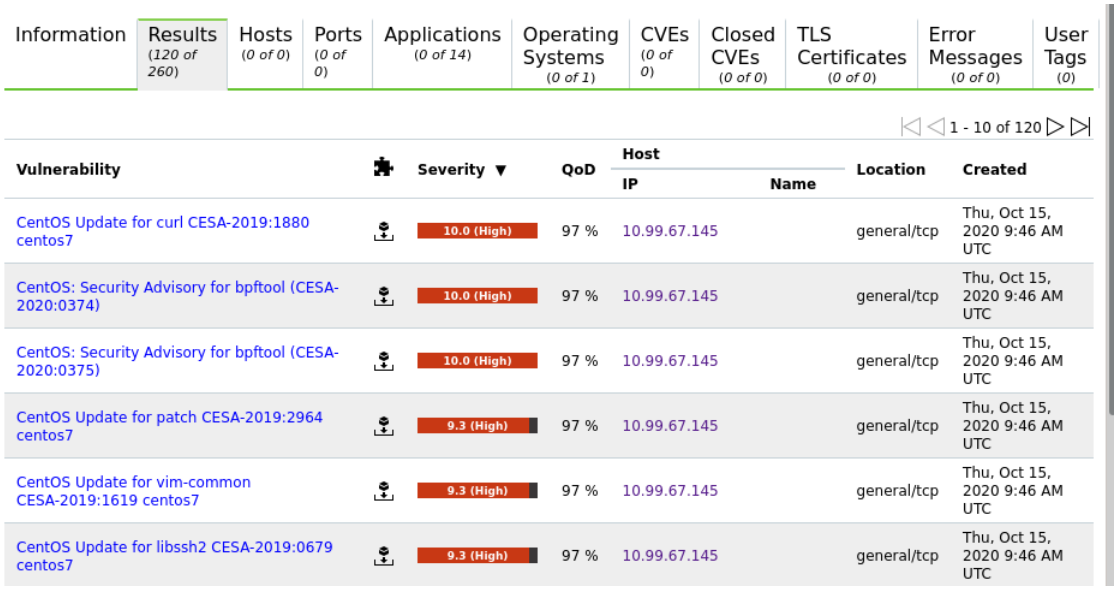
Kuva 14: "Credential" tiedosto

Seuraavaksi tein skannauksen käyttäen luotuja ”credentiaaleja”:



Kuva 15: Credential scan

Saadut tulokset olivat huomattavasti pahemmat kuin normaalissa skannauksessa:



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
CentOS Update for curl CESA-2019:1880 centos7	10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS: Security Advisory for bpftool (CESA-2020:0374)	10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS: Security Advisory for bpftool (CESA-2020:0375)	10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for patch CESA-2019:2964 centos7	9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for vim-common CESA-2019:1619 centos7	9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for libssh2 CESA-2019:0679 centos7	9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC

Haavoittuvuuksien määrä ja vakavuus kasvoi huomattavasti. Kuten kuvasta näkyy haavoittuvuuksien määrä, kasvoi 260:een ja ovat CVSS arvoltaan 10 tai alle. Haavoittuvuus, jonka CVSS arvo on 7-10, on vakava haavoittuvuus, joka pitäisi korjata mahdollisimman pian.

3 Vulnerability analysis

- SELECT 3 different vulnerabilities that you found, and analyze those
  - CVSS metrics – what does it tell?
  - Look at the details of the results – what are the
    - IMPACTS
    - SOLUTIONS
    - VULNERABILITY DETECTION METHODS

Kuva 16: Tehtävänanto 3

3.1 Haavoittuvuus 1

Vulnerability

Name TCP timestamps
Severity 2.6 (Low)
QoD 80 %
Host 10.99.67.145
Location general/tcp

Summary

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

Detection Result

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 8235881
Packet 2: 8236955
```

Insight

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

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP timestamps OID: 1.3.6.1.4.1.25623.1.0.80091

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

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

Solution

Solution Type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the

Kuva 17: TCP timestamp

CVSS eli ”Common Vulnerability Scoring System” on arvo, joka on välillä 0 – 10 ja se kuvastaa haavoittuvuuden vakavuutta. Tämä kyseisen ”TCP timestamp” haavoittuvuuden CVSS arvo on 2.6 (low) mikä on alhainen, eli haavoittuvuuden

vakavuus on lievä. ”TCP timestamp” haavoittuvuus mahdollistaa ”remote hostin” käytettävyysajan muokkaamisen. Ratkaisu tähän on lamauttaa tcp timestamp. Linuxissa täytyy lisätä teksti ”net.ipv4.tcp_timestamp = 0”, /etc/sysctl.conf tiedostoon ja Windowsilla täytyy ajaa komento ”netsh int tcp set global timestamps=disabled”. Haavoittuvuuden voi huomata lähettämällä ”erikois” IP-paketteja pienellä viiveellä ja tutkimalla niiden vastauksia aikaleiman (timestamp) varalta.

3.2 Haavoittuvuus 2

Vulnerability

Name Cleartext Transmission of Sensitive Information via HTTP
Severity 4.8 (Medium)
QoD 80 %
Host 10.99.67.145
Location 80/tcp

Summary

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

Detection Result

```
The following input fields where identified (URL:input name):

http://10.99.67.145/login.php:password
```

Insight

Detection Method

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

Affected Software/OS

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

Impact

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

Solution

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

Kuva 18: Cleartext Transmission via http

Haavoittuvuuden “Cleartext Transmission of Sensitive Information via HTTP” CVSS arvo on 4.8 (medium). “Medium” ja ”low” tason haavoittuvuuden eivät ole vielä hälyttäviä mutta ei niitä pidä myöskään aliarvioida. Tämä kyseinen haavoittuvuus mahdollistaa ”man-in-the-middle” hyökkäyksen käyttäjän ja serverin välillä. Syy tähän on tiedon lähettäminen salaamattomana. Haavoittuvuuden voi huomata, joko tutkimalla liikennettä ja katsomalla onko tieto salattua tai tutkimalla pakottaako

sovellus/”Host” tiedon siirron SSL/TLS yhteydellä. Ratkaisu haavoittuvuuteen on pakottaa sovellukset ja ”hostit” käyttämään SSL/TLS yhteyttä.

3.3 Haavoittuvuus 3

Vulnerability

Name Source Control Management (SCM) Files Accessible
Severity 5.0 (Medium)
QoD 80 %
Host 10.99.67.145
Location 80/tcp

Summary

The script attempts to identify files of a SCM accessible
at the webserver.

Detection Result

```
The following SCM files/folders were identified:

http://10.99.67.145/.git/logs/HEAD
http://10.99.67.145/.git/config
http://10.99.67.145/.git/info/exclude
http://10.99.67.145/.git/description
http://10.99.67.145/.git/HEAD
```

Insight

Currently the script is checking for files of the following SCM:

- Git (.git)

- Mercurial (.hg)

- Bazaar (.bzr)

- CVS (CVS/Root, CVS/Entries)

- Subversion (.svn)

Kuva 19: SCM Files Accessible 1

Detection Method

Check the response if SCM files are accessible.
Details: Source Control Management (SCM) Files Accessible OID: 1.3.6.1.4.1.25623.1.0.111084

Affected Software/OS

Impact

Based on the information provided in this files an attacker might
be able to gather additional info about the structure of the system and its applications.

Solution

Solution Type: Mitigation
Restrict access to the Admin Pages for authorized systems only.

References

Other http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us
https://github.com/anantshri/svn-extractor
https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/

Kuva 20: SCM File Accessible 2

Haavoittuvuuden ”Source Control Management Files Accessible” CVSS arvo on 5 eli keskiverron haavoittuvuus. Haavoittuvuus mahdollistaa järjestelmän rakenteen tutkimisen keräämällä tietoa eri SCM tiedostoista. Ratkaisu tälle on rajoittaa pääsy ”Admin” -sivulle. Kyseisen haavoittuvuuden voi huomata tutkimalla onko SCM tiedostot saavutettavissa.