Network Vulnerability Scan with OpenVAS Report (Light)

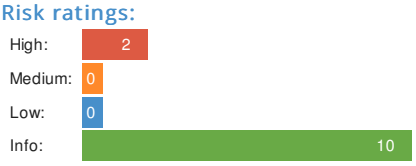
✔ chibaria.com

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2019-11-03 05:49:37 UTC+02
Finish time:	2019-11-03 05:52:27 UTC+02
Scan duration:	2 min, 50 sec
Tests performed:	12/12
Scan status:	Finished

Findings

Vulnerabilities found for Exim Smtpd 4.92 (port 465/tcp)

Risk level	CVSS	CVE	Summary	Exploit
●	10	CVE-2019-15846	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash.	N/A
●	10.0	CVE-2019-13917	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the ${sort } expansion for items that can be controlled by an attacker (e.g., $local_part or $domain).	N/A
●	7.5	CVE-2019-16928	Exim 4.92 through 4.92.2 allows remote code execution, a different vulnerability than CVE-2019-15846. There is a heap-based buffer overflow in string_vformat in string.c involving a long EHLO command.	N/A

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Notes:

- The vulnerabilities are identified based on the server's version information
- Only the highest risk 10 vulnerabilities are shown for each port.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Vulnerabilities found for Exim Smtpd 4.92 (port 587/tcp)

Risk level	CVSS	CVE	Summary	Exploit
●	10	CVE-2019-15846	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash.	N/A
●	10.0	CVE-2019-13917	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the ${sort } expansion for items that can be controlled by an attacker (e.g., $local_part or $domain).	N/A
●	7.5	CVE-2019-16928	Exim 4.92 through 4.92.2 allows remote code execution, a different vulnerability than CVE-2019-15846. There is a heap-based buffer overflow in string_vformat in string.c involving a long EHLO command.	N/A

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Notes:
- The vulnerabilities are identified based on the server's version information
- Only the highest risk 10 vulnerabilities are shown for each port.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

The ports found on the targeted host

Port	State	Service	Product	Product Version	Risk Level
21	open	ftp	Pure-FTPd		● INFO
25	open	smtp			● INFO
53	open	domain	ISC BIND	9.11.4-P2	● INFO
80	open	http	Apache httpd		● INFO
110	open	pop3	Dovecot pop3d		● INFO
143	open	imap	Dovecot imapd		● INFO
443	open	https	Apache httpd		● INFO
465	open	smtp	Exim smtpd	4.92	● HIGH
587	open	smtp	Exim smtpd	4.92	● HIGH
993	open	imaps			● INFO
995	open	pop3s			● INFO

Details

Risk description:
This is the list of ports that have been found open on the target hosts.
Having unnecessary open ports may expose the target systems to inutile risks because those network services and applications may contain vulnerabilities.

Recommendation:

We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

- No vulnerabilities found for port 21 (missing version information)
- No vulnerabilities found for port 25 (missing version information)
- No vulnerabilities found for port 53
- No vulnerabilities found for port 80 (missing version information)
- No vulnerabilities found for port 110 (missing version information)
- No vulnerabilities found for port 143 (missing version information)
- No vulnerabilities found for port 443 (missing version information)
- No vulnerabilities found for port 993 (missing version information)
- No vulnerabilities found for port 995 (missing version information)

Scan coverage information

List of tests performed (12/12)

- ✔ Scanning for open ports...
- ✔ Scanning for vulnerabilities on port: 21 ...
- ✔ Scanning for vulnerabilities on port: 25 ...
- ✔ Scanning for vulnerabilities on port: 53 ...
- ✔ Scanning for vulnerabilities on port: 80 ...
- ✔ Scanning for vulnerabilities on port: 110 ...
- ✔ Scanning for vulnerabilities on port: 143 ...
- ✔ Scanning for vulnerabilities on port: 443 ...
- ✔ Scanning for vulnerabilities on port: 465 ...
- ✔ Scanning for vulnerabilities on port: 587 ...
- ✔ Scanning for vulnerabilities on port: 993 ...
- ✔ Scanning for vulnerabilities on port: 995 ...

Scan parameters

Target:	chibaria.com
Scan type:	Light
Check alive:	False
Protocol type:	Tcp
Ports to scan:	Top 100 ports