

ASSESSMENT REPORT

Services Assessment

Users Assessment

Configurations Assessment

Service Name	CorsairService
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-2018-12441
Exploitability Score	3,9
Impact Score	10
Service Version	3.38.0.4
Severity	HIGH

Service Name	EFS
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-2002-1814
Exploitability Score	3,9
Impact Score	6,4
Service Version	10.0.22621.3235
Severity	MEDIUM

Service Name	MSDTC
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-2002-0224
Exploitability Score	10
Impact Score	2,9
Service Version	2001.12.10941.16384
Severity	MEDIUM

Service Name	Spooler
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-1999-0898
Exploitability Score	3,9
Impact Score	10
Service Version	10.0.22621.3672
Severity	HIGH

Service Name	Steam Client Service
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-2015-4016
Exploitability Score	10
Impact Score	2,9
Service Version	8.98.79.13
Severity	MEDIUM

Service Name	VMnetDHCP
Active Vulnerabilities	Possible Vulnerabilities
CVE	CVE-2019-5540
Exploitability Score	8
Impact Score	2,9
Service Version	16.1.0.683
Severity	MEDIUM

Service Name	VMware NAT Service
--------------	--------------------

Vulnerable Users	High Risk Vulnerable User
TALOS\UserTest	TALOS\TestUser member of Administrators

Service Registry Key	Registry SOFTWARE\Microsoft\Windows\CurrentVersion\Run Needs review
SecurityHealth RtkAudUService	%windir%\system32\SecurityHealthSystray.exe "C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_1803724721d1a34c\RtkAudUService64.exe" -background

Service Configuration File	Apache C:\xampp\apache\conf\httpd - Copy.conf Recommendations Consider adding "ServerTokens Prod" in the configuration file Consider adding "ServerSignature Off" in the configuration file Consider adding "ApacheOptions" in the configuration file Consider adding "Etag" in the configuration file Consider adding "TraceReq" in the configuration file Consider adding "CookieProtection" in the configuration file Consider adding "ClickJacking Attack" in the configuration file Consider adding "X-XSS protection" in the configuration file Consider adding "SSL" in the configuration file Consider adding "Browser Listing" in the configuration file Consider adding "System Setting Protection" in the configuration file Consider adding "HTTP Request Methods Restriction" in the configuration file
Configuration File	C:\xampp\apache\conf\httpd.conf Recommendations Consider adding "ApacheOptions" in the configuration file Consider adding "CookieProtection" in the configuration file Consider adding "SSL" in the configuration file Consider adding "Browser Listing" in the configuration file Consider adding "System Setting Protection" in the configuration file Consider adding "HTTP Request Methods Restriction" in the configuration file

Service Configuration File	Filezilla C:\xampp\FileZillaFTP\FileZilla Server.xml Recommendations
----------------------------	--

ASSESSMENT REPORT

	Active Vulnerabilities	Possible Vulnerabilities
CVE		CVE-2017-4949
Exploitability Score		3,4
Impact Score		10
Service Version		16.1.0.683
Severity		MEDIUM