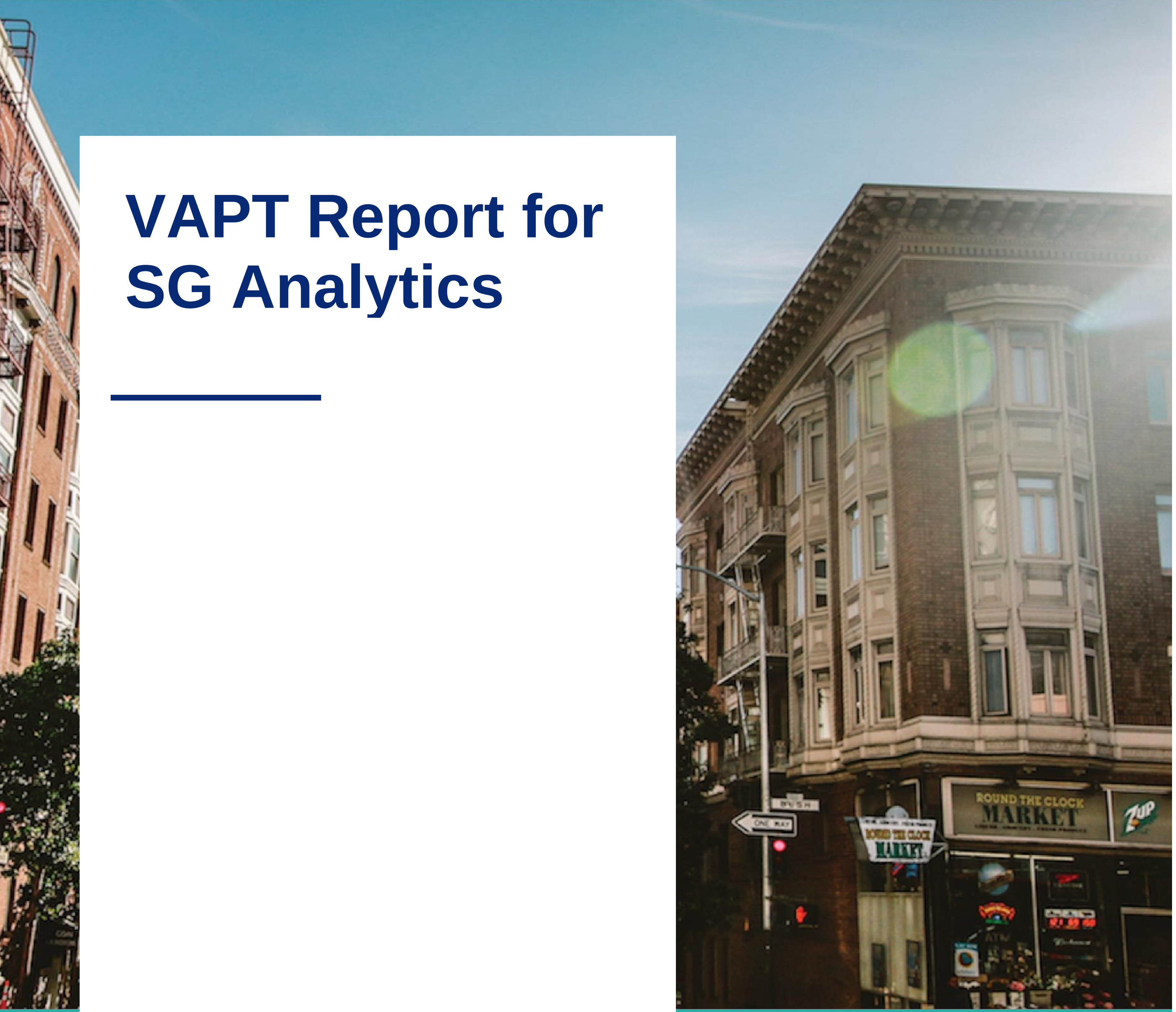
VAPT Report for SG Analytics



AUGUST 27

ProcessLogix Consulting Pvt. Ltd
Authored by: Nikhil Firke

Table of Contents

Executive Summary

This report represents a security audit performed by Nikhil Firke from Processlogix Consulting Pvt Ltd. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

The VAPT audit was conducted in two stages. In first stage, the infrastructure was scanned to identify the as-is state. The stage is used to determine the baseline levels.

Vulnerability Summary

Asset Details			Vulnerabilities					
			Previous			Current		
IP Address	Alias	Operating System	High	Medium	Low	High	Medium	Low
192.168.3.8	-	CentOS Linux	115	193	13	113	202	18
172.16.0.5	-	Linux 3.2	0	8	5	0	8	5
172.16.0.7	TALLY-SERVER	Microsoft Windows Server 2008 Standard Edition SP2	18	33	11	0	1	1
172.16.0.8	MR-SERVER	Microsoft Windows Server 2012 Standard Edition	1	7	6	0	1	2
192.168.1.4	MCAFEE	Microsoft Windows Server 2012 Standard Edition	0	12	9	0	9	9
192.168.1.7	MF-SERVER	Microsoft Windows Server 2012 Standard Edition	1	9	6	0	9	7
192.168.1.9	DLPSRV	Microsoft Windows Server 2012 Standard Edition	1	7	6	0	1	2
192.168.1.11	SGAPUNE1	Microsoft Windows Server 2012 Standard Edition	1	11	9	0	11	9
192.168.1.12	SGAPUNE2	Microsoft Windows Server 2012 Standard Edition	1	11	9	0	11	9
192.168.1.36	SGAWSUS	Microsoft Windows Server 2008 Standard Edition SP2	1	8	5	0	1	3
192.168.10.2	-	Linux 3.2	0	3	5	0	3	5

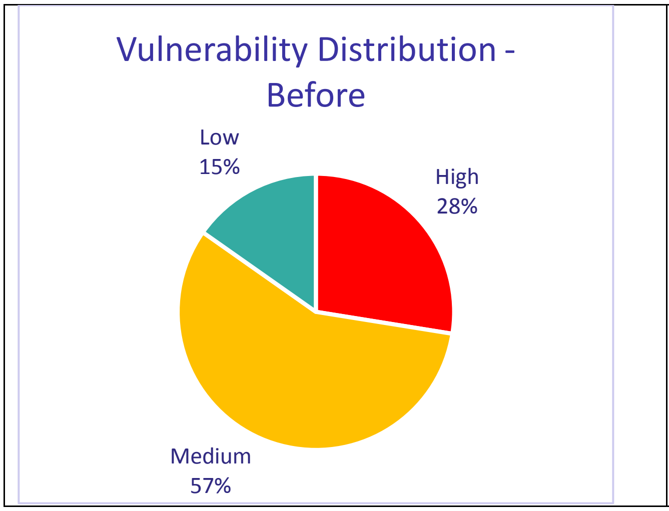
Mitigation Summary

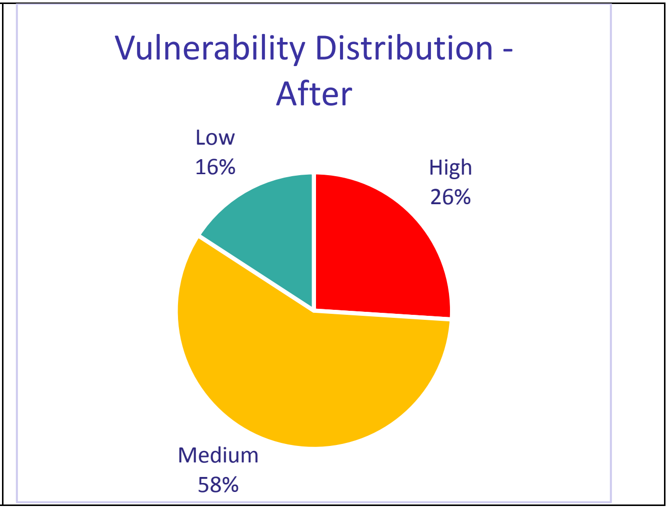
Asset Details	Mitigated Vulnerabilities Percentage		
IP Address	High	Medium	Low
192.168.3.8	NA	-4.66%	-38.46%
172.16.0.5	NA	NA	NA
172.16.0.7	100.00%	96.97%	90.91%
172.16.0.8	100.00%	85.71%	66.67%
192.168.1.4	NA	25.00%	NA
192.168.1.7	100.00%	0	-16.67%
192.168.1.9	100.00%	85.71%	66.67%
192.168.1.11	100.00%	0	0
192.168.1.12	100.00%	0	0
192.168.1.36	100.00%	87.50%	40.00%
192.168.10.2	NA	NA	NA

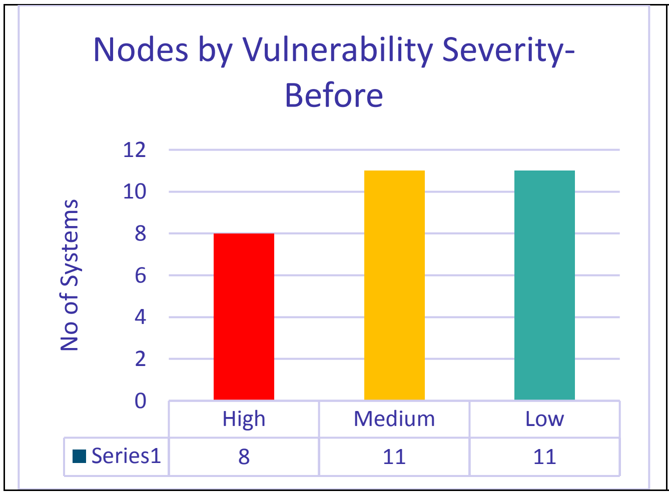
After Mitigation Vulnerability Details

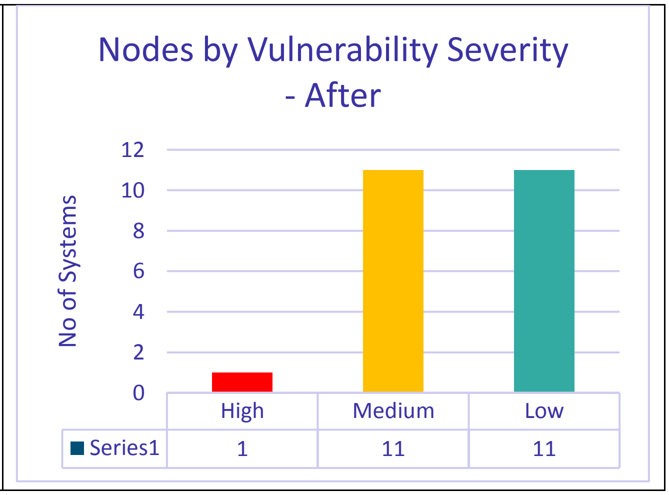
Mitigation Summary Details	Applicable Assets	High	Medium	Low
PHP Vulnerabilities	192.168.3.8	99	154	4
Oracle Vulnerabilities	192.168.3.8	9	8	5
Apache HTTPD Vulnerabilities	192.168.3.8	5	30	1
Cipher Suite Hardening	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.8, 172.16.0.5, 192.168.10.2, 192.168.3.8, 192.168.1.36		10	
SSL Protocol Hardening	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.5, 192.168.10.2, 192.168.3.8		9	
Untrusted Certificates	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.8, 172.16.0.5, 192.168.10.2, 192.168.3.8, 192.168.1.36		9	

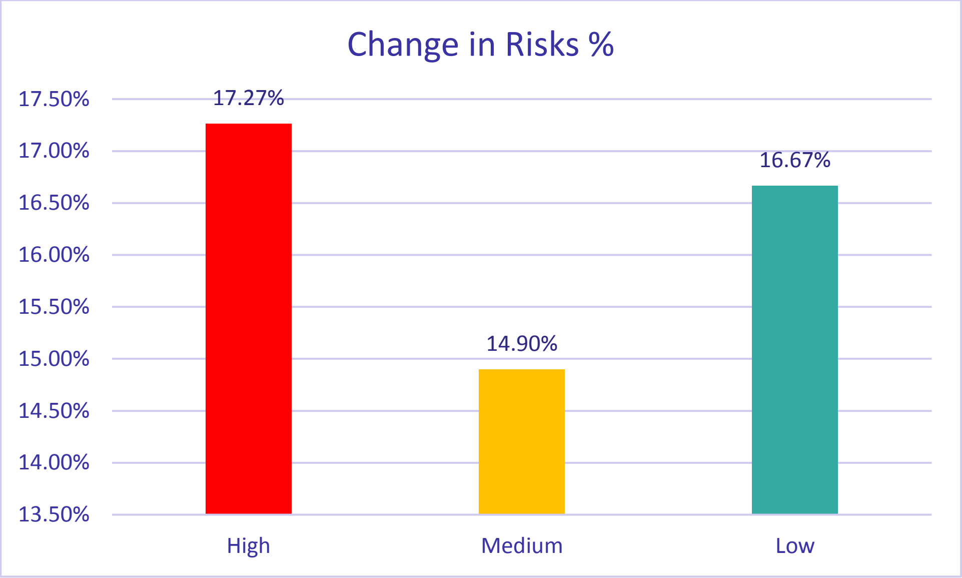
Mitigation Summary Details	Applicable Assets	High	Medium	Low
SMB: Service supports deprecated SMBv1 protocol	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.8, 192.168.1.36		8	
Database Open Access	192.168.3.8, 192.168.1.9		2	
DNS Hardening	192.168.1.11, 192.168.1.12		2	
System Hardening for Web based Settings	192.168.1.9, 192.168.1.4, 192.168.1.7, 172.16.0.5, 192.168.10.2, 192.168.1.36		2	1
ICMP & TCP timestamp response	192.168.3.8, 172.16.0.7			2
UDP IP ID Zero	192.168.3.8			1


Vulnerability Distribution - Before


Vulnerability Distribution - After


Nodes by Vulnerability Severity- Before


Nodes by Vulnerability Severity - After


Change in Risks %
17.50%
17.00%
16.50%
16.00%
15.50%
15.00%
14.50%
14.00%
13.50%
17.27%
14.90%
16.67%
High
Medium
Low

Engagement Details

Objective

The objective of the assessment are as follows

1. Identify the vulnerabilities in the critical nodes in the infrastructure of SG Analytics Pvt. Ltd.
2. Awareness about the baseline mapping of the vulnerability state of the critical processing nodes in SG Analytics infrastructure.

Scope

The IP addresses listed below are identified as critical nodes in SG Analytics infrastructure.
IP Addresses: 192.168.3.8, 172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2

Timelines:

Activity Date	10 July 2019 and 11 July 2019
1st Report Date	15 July 2019
1st Revalidation Date	2 Aug 2019
2nd Revalidation Date	24 Aug 2019
Revalidation Report Date	25 Aug 2019

Remediation Plan Summary

Sr No	Remediation	Applicable IP	Vulnerabilities
1	Upgrade to the latest version of PHP	192.168.3.8	257
2	Upgrade to the latest version of HP System Management Homepage	172.16.0.7	46
3	Apply the Security patches (August 2018) for Oracle Database	192.168.3.8	21
4	Upgrade to the latest version of Apache HTTPD	192.168.3.8	35
5	Disable insecure TLS/SSL protocol support	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	21
6	Obtain a new certificate from your CA and ensure the server configuration is correct	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	9
7	Fix VNC remote control service installed	172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 172.16.0.8,	7
8	Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	8
9	Set the password expiration for Windows Vista/2008 and newer	172.16.0.7, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.8,	5
10	Disable TLS/SSL support for static key cipher suites	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	9

11	Disable TLS/SSL support for RC4 ciphers	172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 172.16.0.8,	7
12	Fix the subject's Common Name (CN) field in the certificate	192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.36	4
13	Disable TLS/SSL support for 3DES cipher suite	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	12
14	Disable HTTP OPTIONS method	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	5
15	Configure SMB signing for Windows	172.16.0.7	3
16	Replace TLS/SSL self-signed certificate	172.16.0.5, 172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 192.168.1.36, 172.16.0.8, 192.168.10.2	9
17	Set an account lockout threshold for Windows Vista/2008 and newer	192.168.1.7, 192.168.1.11, 192.168.1.12	3
18	Secure the SNMP installation	192.168.3.8	2
19	Stop Using SHA-1	172.16.0.7, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 192.168.1.9, 172.16.0.8,	7

MITIGATION DETAILS

Risk Details	PHP Multiple Vulnerabilities
Mitigation	Upgrade to latest version of PHP
Affected Systems	192.168.3.8
Found Instances	257 (99 High, 154 Medium, 4 Low)
Risk Severity	High
Management Response	**We accept this vulnerability. This device is part of our internal infrastructure and not exposed to any external /public network. It's depend on the vendor, once they release security patch will be deployed on the server.** This is embedded device made for specific requirements. This device having customized operating system which is compatible with their own current version. Vendor has already deployed current operating system on this device. Current operating version is Neox_4.0.8.1.
Response Date	

Risk Details	Oracle Multiple Vulnerabilities
Mitigation	Upgrade to latest version of supported Oracle DB with latest patch
Affected Systems	192.168.3.8
Found Instances	22 (9 High, 8 Medium, 5 Low)
Risk Severity	High
Management Response	**We accept this vulnerability. This device is part of our internal infrastructure and not exposed to any external /public network. It's depend on the vendor, once they release security patch will be deployed on the server.** This is embedded device made for specific requirements. This device having customized operating system which is compatible with their own current version. Vendor has already deployed current operating system on this device. Current operating version is Neox_4.0.8.1. Oracle Database default ports are switched to custom ports.
Response Date	

Risk Details	Apache HTTPD Multiple Vulnerabilities
Mitigation	Upgrade to the latest version of Apache HTTPD
Affected Systems	192.168.3.8
Found Instances	36 (5 High, 30 Medium, 1 Low)
Risk Severity	High
Management Response	**We accept this vulnerability. This device is part of our internal infrastructure and not exposed to any external /public network. It's depend on the vendor, once they release security patch will be deployed on the server.**

	This is embedded device made for specific requirements. This device having customized operating system which is compatible with their own current version. Vendor has already deployed current operating system on this device. Current operating version is Neox_4.0.8.1., Custom configuration and tools are developed on the PHP application.
Response Date	

Risk Details	Cipher Suite Hardening
Mitigation	Configure the server to disable support for static key cipher suites. Configure the server to disable support for RC4 ciphers. Configure the server to disable support for 3DES suite. Configure the server to use a randomly generated Diffie-Hellman group Stop using signature algorithms relying on SHA-1, such as "SHA1withRSA" Use a Stronger Key for certificates.
Affected Systems	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.5, 192.168.10.2, 192.168.3.8
Found Instances	10 (10 Medium)
Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning. There ae some dependencies from the OEM side, hence we accept these vulnerabilities** There are custom applications running on these devices i.e. Tally, MacAfee, EPO, DLP, Ad-Connect, if we applied these settings as recommended, its affect product application and services. If we apply these setting on the server there will availability issue of these server. Once the OEM releases security patches it will be deployed on the servers
Response Date	

Risk Details	Insecure TLS/SSL protocol support and Unhardened SSL Protocols
Mitigation	The only option is to disable the affected protocols (SSLv3 and TLS 1.0). Configure the server to require clients to use TLS version 1.2
Affected Systems	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.5, 192.168.10.2, 192.168.3.8
Found Instances	9 (9 Medium)
Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning.** **We need to procure wild card certificate and need to verify commercial.** There are custom applications running on these devices i.e. Tally, MacAfee, EPO, DLP, Ad-Connect, if we applied setting as per recommendation it affects product services. There ae some dependencies from the OEM side. Once it upgraded and released the patch will be deployed on the server

	These devices are part of the internal infrastructure and not exposed to any external /public network
Response Date	

Risk Details	Untrusted or Misconfigured certificates
Mitigation	Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. In addition, ensure the common name (CN) reflects the name of the entity presenting the certificate
Affected Systems	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.5, 192.168.10.2, 192.168.3.8
Found Instances	9 (9 Medium)
Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning. These devices are part of the internal infrastructure and not exposed to any external /public network** **We need to procure wild card certificate and need to verify commercial.** There are custom applications running on these devices with their own certificates, which are provided by the OEM provider and these are their standard certificates.
Response Date	

Risk Details	SMB: Service supports deprecated SMBv1 protocol
Mitigation	Remove/disable SMB1 from domain policy.
Affected Systems	192.168.1.9, 192.168.1.4, 192.168.1.7, 192.168.1.11, 192.168.1.12, 172.16.0.7, 172.16.0.8, 192.168.1.36
Found Instances	8 (8 Medium)
Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning. These devices are part of the internal infrastructure and not exposed to any external /public network** There are custom applications running on these devices, if we applied setting as per recommendation it affects product services and will direct impact on the business process.
Response Date	

Risk Details	Database Open Access
Mitigation	Configure the database server to only allow access to trusted systems.
Affected Systems	192.168.1.9, 192.168.3.8
Found Instances	2 (2 Medium)

Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning. These devices are part of the internal infrastructure and not exposed to any external /public network** Installed application on these devices are compatible with their own database version. if we applied setting as per recommendation it affects product and their services.
Response Date	

Risk Details	DNS Hardening (Query Access on Caching Nameservers)
Mitigation	Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.
Affected Systems	192.168.1.11, 192.168.1.12
Found Instances	2 (2 Medium)
Risk Severity	Medium
Management Response	**We accept this vulnerability, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning. These devices are part of the internal infrastructure and not exposed to any external /public network** We have forward DNS traffic to the ISP DNS for internet access, therefore we cannot restrict/disable it. If we applied setting as per recommendation it will have a major impact on user internet access.
Response Date	

Risk Details	System Hardening for Web based Settings
Mitigation	Disable HTTP OPTIONS, HTTP DELETE method on your web server
Affected Systems	192.168.1.36, 192.168.1.4, 192.168.1.7
Found Instances	3 (2 Medium, 1 Low)
Risk Severity	Medium
Management Response	**We accept this vulnerability.** Installed application on these devices have their own customized certificated / Methods, if we applied setting as per recommendation it will have an impact on accessing applications. These websites installed default IIS service and using their won tool and TCP IP Port for accessing the application. These devices are part of the internal infrastructure and not exposed to any external /public network Additionally, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning, hence we accept these vulnerabilities
Response Date	

Risk Details	NetBIOS NBSTAT Traffic Amplification
Mitigation	Restrict access to the NetBIOS service to only trusted assets.

Affected Systems	172.16.0.7, 172.16.0.8, 192.168.1.4, 192.168.1.9
Found Instances	4 (4 Low)
Risk Severity	Low
Management Response	**We accept this vulnerability.** This required for local network and authorized to SGA authorized devices only. These devices are part of the internal infrastructure and not exposed to any external /public network Additionally, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning, hence we accept these vulnerabilities
Response Date	

Risk Details	Timestamp response
Mitigation	The remote host responded to an ICMP and TCP timestamp request.
Affected Systems	192.168.3.8, 172.16.0.7
Found Instances	2 (2 Low)
Risk Severity	Low
Management Response	**We accept this vulnerability. These ports are required for the internal connectivity and these devices are isolated.** These devices are part of the internal infrastructure and not exposed to any external /public network Additionally, FortiGate 300D firewall gateway is configured to control all level of threat /IPS scanning, hence we accept these vulnerabilities
Response Date	

DETAILED FINDINGS

Discovered Systems

Node	Operating System	Aliases
192.168.3.8	CentOS Linux	
172.16.0.7	Microsoft Windows Server 2008 Standard Edition SP2	TALLY-SERVER
192.168.1.4	Microsoft Windows Server 2012 Standard Edition	MCAFEE
192.168.1.7	Microsoft Windows Server 2012 Standard Edition	• mf-server.sgapune.com MF-SERVER
192.168.1.11	Microsoft Windows Server 2012 Standard Edition	• SGAPUNE1 • SGAPUNE1.SGAPUNE.COM sgapune1.sgapune.com
192.168.1.12	Microsoft Windows Server 2012 Standard Edition	• SGAPUNE2 • sgapune2.sgapune.com SGAPUNE2.SGAPUNE.COM
192.168.1.9	Microsoft Windows Server 2012 Standard Edition	DLPSRV
192.168.1.36	Microsoft Windows Server 2008 Standard Edition SP2	• sgawsus.sgapune.com SGAWSUS
172.16.0.8	Microsoft Windows Server 2012 Standard Edition	MR-SERVER
192.168.10.2	Linux 3.2	
172.168.0.5	Linux 3.2	

Discovered Files and Directories

172.16.0.7

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
C$	Directory	1. comment: Default share mount-point: C:\
Data	Directory	comment:
E$	Directory	1. comment: Default share mount-point: E:\
F$	Directory	1. comment: Default share mount-point: F:\
Finance	Directory	comment:
Finance_CD	Directory	comment:
IT-Fin	Directory	comment:
Project_GT	Directory	comment:
SGA_Finance_Other	Directory	comment:
Shrikant Lanke Backup-01-02-2017	Directory	comment:
Sushant Gupta	Directory	comment:
User backup	Directory	comment:

172.16.0.8

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
Acropolis Copied DVD	Directory	comment:
C$	Directory	1. comment: Default share mount-point: C:\
E$	Directory	1. comment: Default share mount-point: E:\
F$	Directory	1. comment: Default share mount-point: F:\
MR Archived Data	Directory	comment:

File/Directory Name	Type	Properties
MR DATA	Directory	comment:
Market Research Team_new	Directory	comment:
Market Research_DATA	Directory	comment:

192.168.1.11

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
Admin	Directory	comment:
Administrative Staff	Directory	comment:
Audit	Directory	comment:
BSC Data	Directory	comment:
Business Development	Directory	comment:
C$	Directory	1. comment: Default share mount-point: C:\
COE	Directory	comment:
D$	Directory	1. comment: Default share mount-point: D:\
DA_RFP	Directory	comment:
DA_contracts	Directory	comment:
ISO	Directory	comment:
IT	Directory	comment:
Immigration_VISA	Directory	comment:
K$	Directory	1. comment: Default share mount-point: K:\
Learning & Development	Directory	comment:
N$	Directory	1. comment: Default share mount-point: N:\
NETLOGON	Directory	comment: Logon server share
New Transfer	Directory	comment:
Presales	Directory	comment:
Project Data	Directory	comment:
Rhodium	Directory	comment:

File/Directory Name	Type	Properties
SGA Collateral	Directory	comment:
SGA Website	Directory	comment:
SGA_CLIP	Directory	comment:
SGA_Photo	Directory	comment:
SYSVOL	Directory	comment: Logon server share
Screen Saver	Directory	comment:
Survey_Lead_Generation	Directory	comment:
TRSL_KPI_Files	Directory	comment:

192.168.1.12

File/Directory Name	Type	Properties
ADMIN$	Directory	1. comment: Remote Admin mount-point: C:\Windows
C$	Directory	1. comment: Default share mount-point: C:\
D$	Directory	1. comment: Default share mount-point: D:\
Email Archival PST	Directory	1. comment: mount-point: F:\Email Archival PST
F$	Directory	1. comment: Default share mount-point: F:\
HR Team Photo	Directory	1. comment: mount-point: F:\HR Team Photo
IR Data	Directory	1. comment: mount-point: F:\IR Data
L$	Directory	1. comment: Default share mount-point: L:\
NETLOGON	Directory	1. comment: Logon server share mount-point: C:\Windows\SYSVOL\sysvol\SGAPUNE.COM\SCRIPTS
Office_Party_2017	Directory	1. comment: mount-point: F:\Office_Party_2017
Project Data	Directory	1. comment: mount-point: L:\Project Data

File/Directory Name	Type	Properties
SAP Data Backup	Directory	1. comment: mount-point: L:\SAP Data Backup
SYSVOL	Directory	1. comment: Logon server share mount-point: C:\Windows\SYSVOL\sysvol
Tally Server Data Backup	Directory	1. comment: mount-point: L:\Tally Server Data Backup
VIP users Data Backup	Directory	1. comment: mount-point: D:\VIP users Data Backup
VIP_User_Data_BKP	Directory	1. comment: mount-point: L:\VIP_User_Data_BKP
print$	Directory	1. comment: Printer Drivers mount-point: C:\Windows\system32\spool\drivers
prnproc$	Directory	1. comment: Printer Drivers mount-point: C:\Windows\system32\spool\PRTPROCS

192.168.1.36

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
C$	Directory	1. comment: Default share mount-point: C:\
E$	Directory	1. comment: Default share mount-point: E:\
UpdateServicesPackages	Directory	comment: A network share to be used by client systems for collecting all software
WSUSTemp	Directory	comment: A network share used by Local Publishing from a Remote WSUS Console Inst
WsusContent	Directory	comment: A network share to be used by Local Publishing to place published conten
print$	Directory	comment: Printer Drivers
prnproc$	Directory	comment: Printer Drivers

192.168.1.4

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin

File/Directory Name	Type	Properties
C$	Directory	1. comment: Default share mount-point: C:\
D	Directory	comment:
E$	Directory	1. comment: Default share mount-point: E:\
Mcafee	Directory	comment:

192.168.1.7

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
C$	Directory	1. comment: Default share mount-point: C:\
CertEnroll	Directory	comment: Active Directory Certificate Services share
D$	Directory	1. comment: Default share mount-point: D:\
SGA Photos & Videos	Directory	comment:
TRSL Transfer	Directory	comment:
print$	Directory	comment: Printer Drivers

192.168.1.9

File/Directory Name	Type	Properties
ADMIN$	Directory	comment: Remote Admin
C$	Directory	1. comment: Default share mount-point: C:\
D$	Directory	1. comment: Default share mount-point: D:\
Data Analytics Team	Directory	comment:
E$	Directory	1. comment: Default share mount-point: E:\

Services Found

HTTP

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	80	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.11	tcp	8000	0	
192.168.1.12	tcp	80	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	80	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	7777	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.10.2	tcp	1003	1	ssl: true ssl.protocols: tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: false tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,

Device	Protocol	Port	Vulnerabilities	Additional Information
				TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS
192.168.3.8	tcp	80	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false

CIFS

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	139	0	Windows Server (R) 2008 Standard 6.0 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
172.16.0.7	tcp	445	0	Windows Server (R) 2008 Standard 6.0 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required
172.16.0.8	tcp	139	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required

Device	Protocol	Port	Vulnera bilities	Additional Information
				smb1-enabled: true
172.16.0.8	tcp	445	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required
192.168.1.11	tcp	139	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
192.168.1.11	tcp	445	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required
192.168.1.12	tcp	139	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
192.168.1.12	tcp	445	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required
192.168.1.36	tcp	139	0	Windows Server (R) 2008 Standard 6.0

Device	Protocol	Port	Vulnerabilities	Additional Information
				domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
192.168.1.36	tcp	445	0	Windows Server (R) 2008 Standard 6.0 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required
192.168.1.4	tcp	139	2	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: disabled smb1-enabled: true
192.168.1.4	tcp	445	2	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: disabled smb1-enabled: true smb2-enabled: true smb2-signing: enabled
192.168.1.7	tcp	139	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
192.168.1.7	tcp	445	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true

Device	Protocol	Port	Vulnerabilities	Additional Information
				smb2-enabled: true smb2-signing: required
192.168.1.9	tcp	139	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true
192.168.1.9	tcp	445	0	Windows Server 2012 Standard 6.2 domain: SGAPUNE password-mode: encrypt security-mode: user smb-signing: required smb1-enabled: true smb2-enabled: true smb2-signing: required

CIFS Name Service

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes. This service is used to handle CIFS browsing (name) requests. Responses contain the names and types of services that can be accessed via CIFS named pipes.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	udp	137	1	advertised-name-1: TALLY-SERVER (Computer Name) advertised-name-2: SGAPUNE (Domain Name) advertised-name-3: TALLY-SERVER (File Server Service) advertised-name-count: 3 mac-address: 9CB654AF5692
172.16.0.8	udp	137	1	advertised-name-1: MR-SERVER (Computer Name) advertised-name-2: SGAPUNE (Domain Name) advertised-name-3: MR-SERVER (File Server Service) advertised-name-count: 3 mac-address: 9CB654AE3716

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.4	udp	137	1	advertised-name-1: SGAPUNE (Domain Name) advertised-name-2: MCAFEE (Computer Name) advertised-name-3: MCAFEE (File Server Service) advertised-name-count: 3 mac-address: E0071B1B1448
192.168.1.9	udp	137	1	advertised-name-1: DLPSRV (Computer Name) advertised-name-2: SGAPUNE (Domain Name) advertised-name-3: DLPSRV (File Server Service) advertised-name-count: 3 mac-address: 14187761EAC8

DCE Endpoint Resolution

The DCE Endpoint Resolution service, aka Endpoint Mapper, is used on Microsoft Windows systems by Remote Procedure Call (RPC) clients to determine the appropriate port number to connect to for a particular RPC service. This is similar to the portmapper service used on Unix systems.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	135	0	
172.16.0.8	tcp	135	0	
192.168.1.11	tcp	135	0	
192.168.1.11	tcp	593	0	
192.168.1.12	tcp	135	0	
192.168.1.12	tcp	593	0	
192.168.1.36	tcp	135	0	
192.168.1.4	tcp	135	0	
192.168.1.7	tcp	135	0	
192.168.1.9	tcp	135	0	

DCE RPC

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.16.0.7[49152]
172.16.0.7	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:172.16.0.7[49153]
172.16.0.7	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:172.16.0.7[49154]
172.16.0.7	tcp	49155	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.16.0.7[49155]
172.16.0.7	tcp	49190	0	interface-uuid: 6B5BDD1E-528C-422C-AF8C-A4079BE4FE48 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.16.0.7[49190]
172.16.0.7	tcp	49191	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:172.16.0.7[49191]
172.16.0.8	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.16.0.8[49152]
172.16.0.8	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D5 interface-version: 1 name: DHCP Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:172.16.0.8[49153]
172.16.0.8	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:172.16.0.8[49154]

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	49155	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.16.0.8[49155]
172.16.0.8	tcp	49171	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.16.0.8[49171]
172.16.0.8	tcp	49184	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:172.16.0.8[49184]
192.168.1.11	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.11[49152]
192.168.1.11	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.11[49153]
192.168.1.11	tcp	49154	0	interface-uuid: 58E604E8-9ADB-4D2E-A464-3B0683FB1480 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:192.168.1.11[49154]
192.168.1.11	tcp	49155	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.11[49155]
192.168.1.11	tcp	49157	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_http:192.168.1.11[49157]
192.168.1.11	tcp	49158	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.11[49158]
192.168.1.11	tcp	49167	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003

Device	Protocol	Port	Vulnerabilities	Additional Information
				interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.11[49167]
192.168.1.11	tcp	49209	0	interface-uuid: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 interface-version: 5 name: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 protocol-sequence: ncacn_ip_tcp:192.168.1.11[49209]
192.168.1.11	tcp	60684	0	interface-uuid: 897E2E5F-93F3-4376-9C9C-FD2277495C27 interface-version: 1 name: Frs2 Service object-interface-uuid: 5BC1ED07-F5F5-485F-9DFD-6FD0ACF9A23C protocol-sequence: ncacn_ip_tcp:192.168.1.11[60684]
192.168.1.11	tcp	62754	0	interface-uuid: 6B5BDD1E-528C-422C-AF8C-A4079BE4FE48 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:192.168.1.11[62754]
192.168.1.12	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.12[49152]
192.168.1.12	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.12[49153]
192.168.1.12	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:192.168.1.12[49154]
192.168.1.12	tcp	49156	0	interface-uuid: 12345678-1234-ABCD-EF00-01234567CFFB interface-version: 1 name: 12345678-1234-ABCD-EF00-01234567CFFB protocol-sequence: ncacn_ip_tcp:192.168.1.12[49156]
192.168.1.12	tcp	49158	0	interface-uuid: 12345678-1234-ABCD-EF00-01234567CFFB interface-version: 1 name: 12345678-1234-ABCD-EF00-01234567CFFB protocol-sequence: ncacn_ip_tcp:192.168.1.12[49158]
192.168.1.12	tcp	49159	0	interface-uuid: 12345678-1234-ABCD-EF00-01234567CFFB

Device	Protocol	Port	Vulnerabilities	Additional Information
				interface-version: 1 name: 12345678-1234-ABCD-EF00-01234567CFFB protocol-sequence: ncacn_http:192.168.1.12[49159]
192.168.1.12	tcp	50027	0	interface-uuid: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 interface-version: 5 name: 50ABC2A4-574D-40B3-9D66-EE4FD5FBA076 protocol-sequence: ncacn_ip_tcp:192.168.1.12[50027]
192.168.1.12	tcp	53838	0	interface-uuid: 4A452661-8290-4B36-8FBE-7F4093A94978 interface-version: 1 name: Spooler function endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.12[53838]
192.168.1.12	tcp	55274	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.12[55274]
192.168.1.12	tcp	55298	0	interface-uuid: 897E2E5F-93F3-4376-9C9C-FD2277495C27 interface-version: 1 name: Frs2 Service object-interface-uuid: 5BC1ED07-F5F5-485F-9DFD-6FD0ACF9A23C protocol-sequence: ncacn_ip_tcp:192.168.1.12[55298]
192.168.1.36	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.36[49152]
192.168.1.36	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.36[49153]
192.168.1.36	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:192.168.1.36[49154]
192.168.1.36	tcp	49155	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:192.168.1.36[49155]
192.168.1.36	tcp	49172	0	interface-uuid: 12345678-1234-ABCD-EF00-0123456789AB

Device	Protocol	Port	Vulnera bilities	Additional Information
				interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.36[49172]
192.168.1.36	tcp	49185	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.36[49185]
192.168.1.4	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.4[49152]
192.168.1.4	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D5 interface-version: 1 name: DHCP Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.4[49153]
192.168.1.4	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:192.168.1.4[49154]
192.168.1.4	tcp	49155	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.4[49155]
192.168.1.4	tcp	49171	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.4[49171]
192.168.1.4	tcp	58774	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.4[58774]
192.168.1.7	tcp	49152	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.7[49152]
192.168.1.7	tcp	49153	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D5

Device	Protocol	Port	Vulnerabilities	Additional Information
				interface-version: 1 name: DHCP Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.7[49153]
192.168.1.7	tcp	49154	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:192.168.1.7[49154]
192.168.1.7	tcp	49155	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.7[49155]
192.168.1.7	tcp	49181	0	interface-uuid: B25A52BF-E5DD-4F4A-AEA6-8CA7272A0E86 interface-version: 2 name: KeyIso protocol-sequence: ncacn_ip_tcp:192.168.1.7[49181]
192.168.1.7	tcp	49262	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.7[49262]
192.168.1.7	tcp	49308	0	interface-uuid: 91AE6020-9E3C-11CF-8D7C-00AA00C091BE interface-version: 0 name: 91AE6020-9E3C-11CF-8D7C-00AA00C091BE protocol-sequence: ncacn_ip_tcp:192.168.1.7[49308]
192.168.1.9	tcp	1025	0	interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:192.168.1.9[1025]
192.168.1.9	tcp	1026	0	interface-uuid: 3C4728C5-F0AB-448B-BDA1-6CE01EB0A6D6 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.9[1026]
192.168.1.9	tcp	1027	0	interface-uuid: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 interface-version: 1 name: 30B044A5-A225-43F0-B3A4-E060DF91F9C1 protocol-sequence: ncacn_ip_tcp:192.168.1.9[1027]
192.168.1.9	tcp	1028	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1

Device	Protocol	Port	Vulnerabilities	Additional Information
				name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:192.168.1.9[1028]
192.168.1.9	tcp	1047	0	interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:192.168.1.9[1047]
192.168.1.9	tcp	3792	0	interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:192.168.1.9[3792]
192.168.1.9	tcp	6869	0	interface-uuid: 12345678-1234-ABCD-EF00-0123456789AB interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:192.168.1.9[6869]

DNS

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	udp	53	0	
192.168.1.11	tcp	53	0	
192.168.1.11	udp	53	2	
192.168.1.11	tcp	53	1	
192.168.1.12	udp	53	0	
192.168.1.12	tcp	53	0	
192.168.1.12	udp	53	2	
192.168.1.12	tcp	53	1	

FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.12	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.36	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.4	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.7	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	21	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.3.8	tcp	21	0	sslv3: false

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_0: false tlsv1_1: false tlsv1_2: false

HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	80	0	CompuOffice Webserver 2.0.0.0 ASP.NET: 2.0.50727 http.banner: CompuOffice Webserver/2.0.0.0 http.banner.server: CompuOffice Webserver/2.0.0.0
172.16.0.7	tcp	2301	0	HP SMH http.banner: CompaqHTTPServer/9.9 HP System Management Homepage http.banner.server: CompaqHTTPServer/9.9 HP System Management Homepage
172.16.0.7	tcp	5800	0	
172.16.0.7	tcp	8081	0	
172.16.0.8	tcp	5800	0	
172.16.0.8	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
172.16.0.8	tcp	8081	0	
192.168.1.11	tcp	5800	0	

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
192.168.1.11	tcp	8008	0	
192.168.1.11	tcp	8081	0	
192.168.1.12	tcp	5800	0	
192.168.1.12	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
192.168.1.12	tcp	8008	0	
192.168.1.12	tcp	8081	0	
192.168.1.36	tcp	80	2	Microsoft IIS 7.0 .NET CLR: ASP.NET: http.banner: Microsoft-IIS/7.0 http.banner.server: Microsoft-IIS/7.0 http.banner.x-powered-by: ASP.NET verbs-1: GET verbs-2: HEAD verbs-3: OPTIONS verbs-4: POST verbs-5: TRACE verbs-count: 5
192.168.1.36	tcp	5800	0	
192.168.1.36	tcp	8008	0	
192.168.1.36	tcp	8081	0	
192.168.1.4	tcp	80	0	Apache HTTPD http.banner: Apache http.banner.server: Apache
192.168.1.4	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
192.168.1.4	tcp	8008	0	
192.168.1.4	tcp	8081	0	
192.168.1.7	tcp	80	0	Apache HTTPD http.banner: Apache

Device	Protocol	Port	Vulnerabilities	Additional Information
				http.banner.server: Apache
192.168.1.7	tcp	5800	0	
192.168.1.7	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
192.168.1.7	tcp	8008	0	
192.168.1.7	tcp	8081	0	
192.168.1.9	tcp	5800	0	
192.168.1.9	tcp	5985	0	Microsoft-HTTPAPI 2.0 http.banner: Microsoft-HTTPAPI/2.0 http.banner.server: Microsoft-HTTPAPI/2.0
192.168.1.9	tcp	8008	0	
192.168.1.9	tcp	8081	0	
192.168.1.9	tcp	9090	1	verbs-1: GET verbs-2: HEAD verbs-3: OPTIONS verbs-4: POST verbs-count: 4
192.168.3.8	tcp	8008	0	
192.168.3.8	tcp	9090	8	Apache HTTPD 2.2.15 PHP: 5.3.3 http.banner: Apache/2.2.15 (CentOS) http.banner.server: Apache/2.2.15 (CentOS) http.banner.x-powered-by: PHP/5.3.3

HTTPS

HTTPS, the HyperText Transfer Protocol over TLS/SSL, is used to exchange multimedia content on the World Wide Web using encrypted (TLS/SSL) connections. Once the TLS/SSL connection is established, the standard HTTP protocol is used. The multimedia files commonly used with HTTP include text, sound, images and video.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	2381	5	HP SMH http.banner: CompaqHTTPServer/9.9 HP System Management Homepage

Device	Protocol	Port	Vulnerabilities	Additional Information
				http.banner.server: CompaqHTTPServer/9.9 HP System Management Homepage ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Tally-Server.SGAPUNE.COM, OU=Hewlett-Packard Network Management Software (SMH), O=Hewlett-Packard Company, L=Houston, ST=Texas, C=US ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Tue, 03 Feb 2026 11:01:37 IST ssl.cert.not.valid.before: Thu, 04 Feb 2016 11:01:37 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 1454563897 ssl.cert.sha1.fingerprint: 27c31175cf80be4986dd00bdd036b043429a7261 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=Tally-Server.SGAPUNE.COM, OU=Hewlett-Packard Network Management Software (SMH), O=Hewlett-Packard Company, L=Houston, ST=Texas, C=US ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.dh.generator.2048: 2 ssl.dh.prime.2048: ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2261898fa051015728e5a8aacaa68ffffffffffffffff ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: true tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_S

Device	Protocol	Port	Vulnerabilities	Additional Information
				HA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS
192.168.1.4	tcp	443	5	Apache HTTPD http.banner: Apache http.banner.server: Apache ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=AH_CA_McAfee, OU=AH, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Thu, 07 May 2048 16:25:38 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 3832095369235042123 ssl.cert.sha1.fingerprint: 0a066846b71f8cae1c969a0bb0603d7fff26aca8 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=AH_MCAFEE, OU=ePO, O=McAfee ssl.cert.validchain: false ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS
192.168.1.4	tcp	8443	4	Undefined http.banner: Undefined

Device	Protocol	Port	Vulnerabilities	Additional Information
				http.banner.server: Undefined ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Orion_CA_McAfee, OU=Orion, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Fri, 08 May 2048 16:20:50 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 1290207284533956042 ssl.cert.sha1.fingerprint: bc03eb87ac45c4ca8a6956b84455df5df2fc03e5 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=McAfee, OU=Orion, O=McAfee ssl.cert.validchain: false ssl.cert.version: 3 ssl.dh.generator.2048: 3fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af2767164e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664b4c0f6cc41659 ssl.dh.prime.2048: 87a8e61db4b6663cffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f26375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a1597 ssl.protocols: tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: false tlsv1_1: true

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS verbs-1: DELETE verbs-2: GET verbs-3: HEAD verbs-4: OPTIONS verbs-5: POST verbs-6: PUT verbs-count: 6
192.168.1.4	tcp	8444	5	Undefined http.banner: Undefined http.banner.server: Undefined ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Orion_CA_McAfee, OU=Orion, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Thu, 07 May 2048 16:20:52 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 8984522399286579276 ssl.cert.sha1.fingerprint: 6e26a0634cb5125b51cbc567995e82adf37e2d30 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=Orion_ClientAuth_McAfee, OU=Orion, O=McAfee

Device	Protocol	Port	Vulnerabilities	Additional Information
				ssl.cert.validchain: false ssl.cert.version: 3 ssl.dh.generator.2048: 3fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af2767164e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664b4c0f6cc41659 ssl.dh.prime.2048: 87a8e61db4b6663cffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f26375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a1597 ssl.protocols: tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: false tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_2

Device	Protocol	Port	Vulnerabilities	Additional Information
				56_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS verbs-1: DELETE verbs-2: GET verbs-3: HEAD verbs-4: OPTIONS verbs-5: POST verbs-6: PUT verbs-count: 6
192.168.1.7	tcp	443	6	Apache HTTPD http.banner: Apache http.banner.server: Apache ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=AH_CA_MF-Server, OU=AH, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Thu, 15 Feb 2046 13:23:00 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 8945450869219933310 ssl.cert.sha1.fingerprint: 213096218ede074f1614904b1b7a32eba33853b7 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=AH_MF-SERVER, OU=ePO, O=McAfee ssl.cert.validchain: false ssl.cert.version: 3 ssl.dh.generator.2048: 2 ssl.dh.prime.2048: ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2261898fa051015728e5a8aacaa68ffffffffffffffff ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2

Device	Protocol	Port	Vulnerabilities	Additional Information
				sslv2: false sslv3: false tlsv1_0: true tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_CAMELLIA_256_CBC_

Device	Protocol	Port	Vulnerabilities	Additional Information
				SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS
192.168.1.7	tcp	8443	5	Undefined http.banner: Undefined http.banner.server: Undefined ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Orion_CA_MF-Server, OU=Orion, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Wed, 14 Feb 2046 18:58:07 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 8819501996760114324 ssl.cert.sha1.fingerprint: 275538585e701e2ad63ea580041b5388ea33d37d ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=MF-Server, OU=Orion, O=McAfee ssl.cert.validchain: false ssl.cert.version: 3 ssl.dh.generator.2048: 3fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af2767164e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664b4c0f6cc41659 ssl.dh.prime.2048: 87a8e61db4b6663cffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8

Device	Protocol	Port	Vulnerabilities	Additional Information
				ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f26375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a1597 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: true tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS verbs-1: DELETE verbs-2: GET verbs-3: HEAD

Device	Protocol	Port	Vulnerabilities	Additional Information
				verbs-4: OPTIONS verbs-5: POST verbs-6: PUT verbs-count: 6
192.168.1.7	tcp	8444	6	Undefined http.banner: Undefined http.banner.server: Undefined ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Orion_CA_MF-Server, OU=Orion, O=McAfee ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Wed, 14 Feb 2046 17:36:44 IST ssl.cert.not.valid.before: Thu, 01 Jan 1970 05:30:00 IST ssl.cert.selfsigned: false ssl.cert.serial.number: 2862223203528278227 ssl.cert.sha1.fingerprint: 9bc445b9d6d5a02eb89c0b377eead2dea93f4ab9 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=Orion_ClientAuth_MF-Server, OU=Orion, O=McAfee ssl.cert.validchain: false ssl.cert.version: 3 ssl.dh.generator.2048: 3fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af2767164e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664b4c0f6cc41659 ssl.dh.prime.2048: 87a8e61db4b6663cffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f26375d7014

Device	Protocol	Port	Vulnerabilities	Additional Information
				103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a1597 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: true tlsv1_0.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_0.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS verbs-1: DELETE verbs-2: GET verbs-3: HEAD verbs-4: OPTIONS verbs-5: POST

Device	Protocol	Port	Vulnerabilities	Additional Information
				verbs-6: PUT verbs-count: 6
192.168.1.9	tcp	443	5	Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 http.banner.server: Apache-Coyote/1.1 ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=localhost, O=Symantec Corp., L=San Francisco, ST=CA, C=US ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Tue, 14 Feb 2023 03:10:44 IST ssl.cert.not.valid.before: Sat, 16 Feb 2013 03:10:44 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 190721684 ssl.cert.sha1.fingerprint: d8f6021df4e305e079a10ecbe1303d7f87c07029 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=localhost, O=Symantec Corp., L=San Francisco, ST=CA, C=US ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.10.2	tcp	443	4	xxxxxxxx-xxxxx

Device	Protocol	Port	Vulnerabilities	Additional Information
				http.banner: xxxxxxxx-xxxxx http.banner.server: xxxxxxxx-xxxxx ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=FGT3HD3914801558, O=Fortinet Ltd. ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Sat, 16 Dec 2028 08:10:42 IST ssl.cert.not.valid.before: Sun, 16 Dec 2018 08:10:42 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 2848257963348762037 ssl.cert.sha1.fingerprint: eb4fe668f0dd3ad1b41e825c51be9ae781d56bd0 ssl.cert.sig.alg.name: SHA256withRSA ssl.cert.subject.dn: CN=FGT3HD3914801558, O=Fortinet Ltd. ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.dh.generator.2048: 2 ssl.dh.prime.2048: ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca18217c32905e462e36ce3be39e772c180e86039b2783a2ec07a28fb5c55df06f4c52c9de2bcbf6955817183995497cea956ae515d2261898fa051015728e5a8aacaa68ffffffffffffffff ssl.protocols: tlsv1_1,tlsv1_2 sslv2: false sslv3: false tlsv1_0: false tlsv1_1: true tlsv1_1.TLS_DHE_RSA_WITH_AES_128_CBC_SHA.dh.keysize: 2048 tlsv1_1.TLS_DHE_RSA_WITH_AES_256_CBC_SHA.dh.keysize: 2048 tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS verbs-1: GET verbs-2: HEAD verbs-3: OPTIONS verbs-count: 3

IMAP

IMAP, the Interactive Mail Access Protocol or Internet Message Access Protocol, is used to access and manipulate electronic mail (e-mail). IMAP servers can contain several folders, aka mailboxes, containing messages (e-mails) for users.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.12	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.36	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.4	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.7	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.3.8	tcp	143	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false

Kerberos

Kerberos is a network authentication and encryption protocol. A client will first authenticate itself to a Kerberos server, in other words, using some shared secret information, the client first proves to the server that he is actually who he says he is and that he is allowed access to the specified systems he is asking to use. A Kerberos server has domain over a specific set of servers and services, and if the client can be authenticated the server provides the client with a ticket, allowing him to access the requested services. Kerberos provides support for renewing and extending the scope of that ticket. In addition, once the client has obtained a ticket, all data sent between the client and other Kerberos protected services are strongly encrypted. This prevents malicious eavesdropping or non-authenticated clients from hijacking established sessions. Kerberos also has a secure password administration protocol that operates on a different port that the main Kerberos authentication protocol.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	88	0	
192.168.1.11	tcp	464	0	
192.168.1.12	tcp	88	0	

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.12	tcp	464	0	

LDAP

LDAP, the Lightweight Directory Access Protocol, is used to access and manipulate X.500 directories. X.500 directories are often used to store user information for an organization, including full name, e-mail address, phone numbers, etc.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	389	0	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711081420.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE1.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 122416907 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune1$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4
192.168.1.11	tcp	3268	0	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711081420.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE1.SGAPUNE.COM domainControllerFunctionality: 5

Device	Protocol	Port	Vulnerabilities	Additional Information
				domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 122416907 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune1$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4
192.168.1.12	tcp	389	0	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711082237.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE2.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 91945106 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune2$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				serverName: CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4
192.168.1.12	tcp	3268	0	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				currentTime: 20190711082237.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE2.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 91945106 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune2$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4

LDAPS

LDAPS, the Lightweight Directory Access Protocol over TLS/SSL, is used to access and manipulate X.500 directories using encrypted(TLS/SSL) connections. X.500 directories are often used to store user information for an organization, including full name, e-mail address, phone numbers, etc.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	636	4	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711081420.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE1.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				forestFunctionality: 5 highestCommittedUSN: 122416907 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune1$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM ssl: true ssl.protocols: sslv3,tlsv1_0,tlsv1_1,tlsv1_2 sslv3: true sslv3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 sslv3.extensions: RENEGOTIATION_INFO subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4 tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS

Device	Protocol	Port	Vulnerabilities	Additional Information
				_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.11	tcp	3269	4	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711081420.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE1.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 122416907 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune1$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM ssl: true ssl.protocols: sslv3,tlsv1_0,tlsv1_1,tlsv1_2 sslv3: true sslv3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 sslv3.extensions: RENEGOTIATION_INFO subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4 tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_

Device	Protocol	Port	Vulnerabilities	Additional Information
				SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.12	tcp	636	4	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711082237.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE2.SGAPUNE.COM domainControllerFunctionality: 5 domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 91945106 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune2$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM

Device	Protocol	Port	Vulnerabilities	Additional Information
				namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM ssl: true ssl.protocols: sslv3,tlsv1_0,tlsv1_1,tlsv1_2 sslv3: true sslv3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 sslv3.extensions: RENEGOTIATION_INFO subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338 supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4 tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.12	tcp	3269	4	configurationNamingContext: CN=Configuration,DC=SGAPUNE,DC=COM currentTime: 20190711082237.0Z defaultNamingContext: DC=SGAPUNE,DC=COM dnsHostName: SGAPUNE2.SGAPUNE.COM domainControllerFunctionality: 5

Device	Protocol	Port	Vulnerabilities	Additional Information
				domainFunctionality: 5 dsServiceName: CN=NTDS Settings,CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM forestFunctionality: 5 highestCommittedUSN: 91945106 isGlobalCatalogReady: TRUE isSynchronized: TRUE ldap.anonymous.access.enabled: false ldapServiceName: SGAPUNE.COM:sgapune2$@SGAPUNE.COM namingContexts-1: DC=SGAPUNE,DC=COM namingContexts-2: CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-3: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM namingContexts-4: DC=DomainDnsZones,DC=SGAPUNE,DC=COM namingContexts-5: DC=ForestDnsZones,DC=SGAPUNE,DC=COM namingContexts-count: 5 rootDomainNamingContext: DC=SGAPUNE,DC=COM schemaNamingContext: CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM serverName: CN=SGAPUNE2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=SGAPUNE,DC=COM ssl: true ssl.protocols: sslv3,tlsv1_0,tlsv1_1,tlsv1_2 sslv3: true sslv3.ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 sslv3.extensions: RENEGOTIATION_INFO subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=SGAPUNE,DC=COM supportedCapabilities-1: 1.2.840.113556.1.4.800 supportedCapabilities-2: 1.2.840.113556.1.4.1670 supportedCapabilities-3: 1.2.840.113556.1.4.1791 supportedCapabilities-4: 1.2.840.113556.1.4.1935 supportedCapabilities-5: 1.2.840.113556.1.4.2080 supportedCapabilities-6: 1.2.840.113556.1.4.2237 supportedCapabilities-count: 6 supportedControl-1: 1.2.840.113556.1.4.319 supportedControl-10: 1.2.840.113556.1.4.521 supportedControl-11: 1.2.840.113556.1.4.970 supportedControl-12: 1.2.840.113556.1.4.1338

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedControl-13: 1.2.840.113556.1.4.474 supportedControl-14: 1.2.840.113556.1.4.1339 supportedControl-15: 1.2.840.113556.1.4.1340 supportedControl-16: 1.2.840.113556.1.4.1413 supportedControl-17: 2.16.840.1.113730.3.4.9 supportedControl-18: 2.16.840.1.113730.3.4.10 supportedControl-19: 1.2.840.113556.1.4.1504 supportedControl-2: 1.2.840.113556.1.4.801 supportedControl-20: 1.2.840.113556.1.4.1852 supportedControl-21: 1.2.840.113556.1.4.802 supportedControl-22: 1.2.840.113556.1.4.1907 supportedControl-23: 1.2.840.113556.1.4.1948 supportedControl-24: 1.2.840.113556.1.4.1974 supportedControl-25: 1.2.840.113556.1.4.1341 supportedControl-26: 1.2.840.113556.1.4.2026 supportedControl-27: 1.2.840.113556.1.4.2064 supportedControl-28: 1.2.840.113556.1.4.2065 supportedControl-29: 1.2.840.113556.1.4.2066 supportedControl-3: 1.2.840.113556.1.4.473 supportedControl-30: 1.2.840.113556.1.4.2090 supportedControl-31: 1.2.840.113556.1.4.2205 supportedControl-32: 1.2.840.113556.1.4.2204 supportedControl-33: 1.2.840.113556.1.4.2206 supportedControl-34: 1.2.840.113556.1.4.2211 supportedControl-35: 1.2.840.113556.1.4.2239 supportedControl-4: 1.2.840.113556.1.4.528 supportedControl-5: 1.2.840.113556.1.4.417 supportedControl-6: 1.2.840.113556.1.4.619 supportedControl-7: 1.2.840.113556.1.4.841 supportedControl-8: 1.2.840.113556.1.4.529 supportedControl-9: 1.2.840.113556.1.4.805 supportedControl-count: 35 supportedExtension-1: 1.3.6.1.4.1.1466.20037 supportedExtension-2: 1.3.6.1.4.1.1466.101.119.1 supportedExtension-3: 1.2.840.113556.1.4.1781 supportedExtension-4: 1.3.6.1.4.1.4203.1.11.3 supportedExtension-5: 1.2.840.113556.1.4.2212 supportedExtension-count: 5 supportedLDAPPolicies-1: MaxPoolThreads supportedLDAPPolicies-10: MaxTempTableSize

Device	Protocol	Port	Vulnerabilities	Additional Information
				supportedLDAPPolicies-11: MaxResultSetSize supportedLDAPPolicies-12: MinResultSets supportedLDAPPolicies-13: MaxResultSetsPerConn supportedLDAPPolicies-14: MaxNotificationPerConn supportedLDAPPolicies-15: MaxValRange supportedLDAPPolicies-16: ThreadMemoryLimit supportedLDAPPolicies-17: SystemMemoryLimitPercent supportedLDAPPolicies-2: MaxDatagramRecv supportedLDAPPolicies-3: MaxReceiveBuffer supportedLDAPPolicies-4: InitRecvTimeout supportedLDAPPolicies-5: MaxConnections supportedLDAPPolicies-6: MaxConnIdleTime supportedLDAPPolicies-7: MaxPageSize supportedLDAPPolicies-8: MaxBatchReturnMessages supportedLDAPPolicies-9: MaxQueryDuration supportedLDAPPolicies-count: 17 supportedLDAPVersion-1: 3 supportedLDAPVersion-2: 2 supportedLDAPVersion-count: 2 supportedSASLMechanisms-1: GSSAPI supportedSASLMechanisms-2: GSS-SPNEGO supportedSASLMechanisms-3: EXTERNAL supportedSASLMechanisms-4: DIGEST-MD5 supportedSASLMechanisms-count: 4 tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO

MySQL

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.3.8	tcp	3306	1	Oracle MySQL mysql.error: Host '192.168.3.2' is not allowed to connect to this MySQL server

NNTP

The Network News Transfer Protocol provides a means for the retrieval, distribution, posting and searching of messages, referred to as news articles. The service provided allows for the storage of these news articles in a central database, and provides methods for clients to select only the articles that are needed. This protocol provides a suite of commands that allow a user to list the articles available to read, search through those articles, and post new content to a specific news database. The news service also has support for cross-referencing news articles with each other, and the expiration and removal of old and outdated content.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.12	tcp	119	0	sslv3: false tlsv1_0: false

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_1: false tlsv1_2: false
192.168.1.36	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.4	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.7	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.3.8	tcp	119	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false

NTP

The Network Time Protocol (NTP) is used to keep the clocks of machines on a network synchronized. Provisions are made in the protocol to account for network disruption and packet latency.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	udp	123	0	
192.168.1.12	udp	123	0	

Oracle TNS Listener

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.9	tcp	1521	1	Oracle Database 11.2.0.4
192.168.3.8	tcp	1521	10	Oracle Database 10.2.0.1

POP

The Post Office Protocol allows workstations to retrieve e-mail dynamically from a mailbox server.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.12	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.36	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.4	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.7	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.3.8	tcp	110	0	sslv3: false tlsv1_0: false tlsv1_1: false

Device	Protocol	Port	Vulnerabilities	Additional Information
				tlsv1_2: false

RDP

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	3389	3	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=Tally-Server.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Fri, 16 Aug 2019 12:20:39 IST ssl.cert.not.valid.before: Thu, 14 Feb 2019 12:20:39 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 39371674884995966983965287782657685587 ssl.cert.sha1.fingerprint: 5541905b7e27f1a4f176c76930ea5a99369e3645 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=Tally-Server.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 ssl.supportsInsecureRenegotiation: true sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: tlsv1_1: true tlsv1_1.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions:

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.8	tcp	3389	5	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=MR-Server.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Tue, 01 Oct 2019 15:29:09 IST ssl.cert.not.valid.before: Mon, 01 Apr 2019 15:29:09 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 123795229111360195672758391695001681519 ssl.cert.sha1.fingerprint: 8eb2b369ba59f30952efef41d81a30b443b0fd05 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=MR-Server.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CB

Device	Protocol	Port	Vulnerabilities	Additional Information
				C_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.11	tcp	3389	5	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=SGAPUNE1.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Tue, 07 Jan 2020 02:14:12 IST ssl.cert.not.valid.before: Mon, 08 Jul 2019 02:14:12 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 39540608754537021304244752761243712703 ssl.cert.sha1.fingerprint: 78322730ea51ea5c3aa923b2962ea586245006e0 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=SGAPUNE1.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SH

Device	Protocol	Port	Vulnerabilities	Additional Information
				A384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.12	tcp	3389	5	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=SGAPUNE2.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Mon, 12 Aug 2019 15:29:26 IST ssl.cert.not.valid.before: Sun, 10 Feb 2019 15:29:26 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 151697595768872580077345199583076831514 ssl.cert.sha1.fingerprint: 7e56d5e2c93a3f58eb4c727135b2a375fa8d4235 ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=SGAPUNE2.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA

Device	Protocol	Port	Vulnerabilities	Additional Information
				_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO
192.168.1.36	tcp	3389	3	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=SGAWSUS.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Thu, 26 Dec 2019 12:12:05 IST ssl.cert.not.valid.before: Wed, 26 Jun 2019 12:12:05 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 49450618008622752508361860368127130666 ssl.cert.sha1.fingerprint: 758531037cd5ce74d6d36db1a0cbc5a459ca74fa ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=SGAWSUS.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 ssl.supportsInsecureRenegotiation: true sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: tlsv1_1: true tlsv1_1.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA tlsv1_2.extensions:
192.168.1.4	tcp	3389	5	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors]

Device	Protocol	Port	Vulnerabilities	Additional Information
				ssl.cert.issuer.dn: CN=McAfee.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Sun, 22 Sep 2019 03:30:35 IST ssl.cert.not.valid.before: Sat, 23 Mar 2019 03:30:35 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 43695820880214749081871101059327408786 ssl.cert.sha1.fingerprint: 91e020db0106effd562f875e1746c3826dc1726f ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=McAfee.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.7	tcp	3389	5	ssl: true ssl.cert.chainerror: [Path does not chain with any of the trust anchors] ssl.cert.issuer.dn: CN=MF-Server.SGAPUNE.COM ssl.cert.key.alg.name: RSA ssl.cert.key.rsa.modulusBits: 2048 ssl.cert.not.valid.after: Mon, 16 Dec 2019 03:51:07 IST ssl.cert.not.valid.before: Sun, 16 Jun 2019 03:51:07 IST ssl.cert.selfsigned: true ssl.cert.serial.number: 86682475722866888585278208427273135495 ssl.cert.sha1.fingerprint: fa8df8c9c4a67c373dcd855b1582aa320ef1d87c ssl.cert.sig.alg.name: SHA1withRSA ssl.cert.subject.dn: CN=MF-Server.SGAPUNE.COM ssl.cert.validchain: false ssl.cert.validsignature: true ssl.cert.version: 3 ssl.protocols: tlsv1_0,tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: true tlsv1_0.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_0.extensions: RENEGOTIATION_INFO tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_1.extensions: RENEGOTIATION_INFO tlsv1_2: true tlsv1_2.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CB

Device	Protocol	Port	Vulnerabilities	Additional Information
				C_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5 tlsv1_2.extensions: RENEGOTIATION_INFO

RTSP

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.9	tcp	7070	0	Eclipse Jetty 9.2.z-SNAPSHOT http.banner: Jetty(9.2.z-SNAPSHOT) http.banner.server: Jetty(9.2.z-SNAPSHOT)

SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.1.11	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.12	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.36	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.4	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.7	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.1.9	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false
192.168.3.8	tcp	25	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false

SNMP

Simple Network Management Protocol (SNMP), like the name implies, is a simple protocol used to manage networking appliances by remote clients. It is primarily UDP-based and uses trivial authentication by means of a secret community name.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.3.8	udp	161	2	assignedNumber: 99 snmp.banner: SNMPv3 agent from SNMP Research, Inc. snmp.contact: Clarent Support snmp.location: Clarent VOIP Lab snmp.sysObjectID: 1.3.6.1.4.1.99.1.1.3.1 snmp.uptime: 315 days, 14:16:09.49 sysDescr: SNMPv3 agent from SNMP Research, Inc.

SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.10.2	tcp	222	0	ssh.banner: SSH-2.0-H5x7_Ki_jfN6a ssh.protocol.version: 2.0 ssh.rsa.pubkey.fingerprint: 5EB697DAF2520FC352FA8E48BDA6FB88

VNC

AT&T VNC is used to provide graphical control of a system. A VNC server can run on a Microsoft Windows, Apple Macintosh or Unix (X Windows) system. By supplying the appropriate password, a VNC server system can be accessed by a VNC client. Full control of the system is provided through VNC, including command execution.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
172.16.0.7	tcp	5900	1	protocol-version: 3.8 supported-auth-1: VNC Authentication supported-auth-2: Tight supported-auth-count: 2
172.16.0.8	tcp	5900	1	
192.168.1.11	tcp	5900	1	protocol-version: 3.8 supported-auth-1: VNC Authentication

Device	Protocol	Port	Vulnerabilities	Additional Information
				supported-auth-2: Tight supported-auth-count: 2
192.168.1.12	tcp	5900	1	
192.168.1.36	tcp	5900	1	protocol-version: 3.8 supported-auth-1: VNC Authentication supported-auth-2: Tight supported-auth-count: 2
192.168.1.7	tcp	5900	1	protocol-version: 3.8 supported-auth-1: VNC Authentication supported-auth-2: Tight supported-auth-count: 2
192.168.1.9	tcp	5900	1	protocol-version: 3.8 supported-auth-1: VNC Authentication supported-auth-2: Tight supported-auth-count: 2

cadlock

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.10.2	tcp	1000	1	ssl: true ssl.protocols: tlsv1_1,tlsv1_2 sslv3: false tlsv1_0: false tlsv1_1: true tlsv1_1.ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA tlsv1_1.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS tlsv1_2: true tlsv1_2.ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TL

Device	Protocol	Port	Vulnerabilities	Additional Information
				S_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256 tlsv1_2.extensions: RENEGOTIATION_INFO,EC_POINT_FORMATS

portmapper

The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.3.8	udp	111	0	program-number: 100000 program-version: 2
192.168.3.8	tcp	111	0	program-number: 100000 program-version: 2