Vulnerability Assessment

Executive Summary Report

Customer NAME

Wednesday, November 10, 2021

Document details

Document

Title	Vulnerability Assessment
Subtitle	Executive Summary
Classification	Confidential

Document Version

Version	Date	Changes	Author (s)
0.1	02.11.2021	Initial Document	Sebastian Eitel
0.2	03.11.2021	Internally Reviewed	Brian Verburg
0.3			

Contact information

Name	Sebastian Eitel
Function	Cyber Security Architect
E-mail address	Sebastian.Eitel@ingrammicro.com

Disclaimer

Contents

1 Introduction

Ingram Micro Center of Excellence for Cybersecurity conducted a Vulnerability Assessment of CustomerName by in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use.

This document is the Executive Summary. Detailed information about the identified issues, their potential impact and recommended actions can be found in the detailed report Documents for each network segment.

It is strongly recommended to fix the findings and do a Vulnerability Assessment on a recurring basis.

1.1 Scope of the testing

The Vulnerability Assessment was performed on the organization's assets. The assessment utilized industry-standard Vulnerability Scanner tools and frameworks. The following table summarizes the scope of type of testing performed:

Name of organization	CustomerName
Type of Test	Vulnerability Assessment
Security Assessment performed by	Ingram Micro Center of Excellence for Cyber Security
IP Addresses	192.168.x.0/23 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 192.168.x.0/24 10.10.x.0/24 10.10.x.0/24
Duration of Assessment	x Days
Starting Date	xx.xx.xxxx

1.2 Severity Definitions

A qualitative impact factor (Critical, High, Medium, or Low) has been associated with each vulnerability.

Activity's severity categorizations are illustrated in the table below:

Risk Rating	Description
CRITICAL	High Severity issues that can be exploited in isolation, with no additional steps necessary, that may provide total compromise of the system.
HIGH	Severe issues that can easily be exploited to immediately impact the environment.
MEDIUM	Moderate security issues that require some effort to successfully influence the environment.
LOW	Security issues that have a limited or trivial impact to the environment.
INFORMATIONAL	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

2 Executive Summary

2.1 Summary of findings

The below table present summarized information about the discovered vulnerabilities, misconfiguration, and weaknesses.

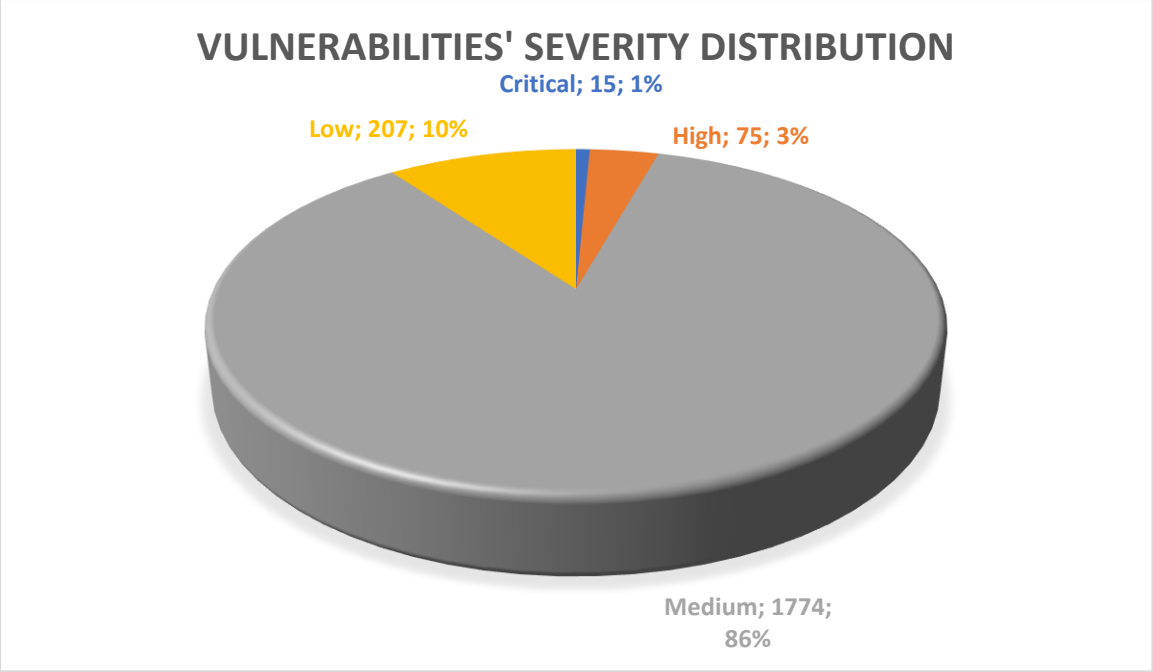
Detailed information about the identified issues, their potential impact and recommended actions can be found in the detailed report Documents for each network segment.

Top Level Overview							
Scan	**Targets**		**Critical**	**High**	**Medium**	**Low**	
Company Network	621		15	75	1774	207	

Vulnerabilities by Network and Risk Level							
Network	**Targets**		**Critical**	**High**	**Medium**	**Low**	
192.168.x.0/23	463		6	34	685	70	
192.168.x.0/24	8		-	-	27	274	
192.168.x.0/24	8		-	-	115	1	
192.168.x.0/24	39		2	15	142	75	
192.168.x.0/24	16		-	2	388	4	
192.168.x.0/24	8		-	1	19	-	
192.168.x.0/24	47		6	11	180	33	
192.168.x.0/24	17		-	2	55	2	
10.10.x.0/24	9		-	2	97	7	
10.10.x.0/24	6		1	8	166	15	

Risk by Vulnerabilities		
Severity	Vulnerabilities	Unique
Informational	14980	187
Low	207	10
Medium	1774	46
High	75	12
Critical	15	5

Risk by Hosts	
Severity	Number of hosts
Informational	621
Low	84
Medium	188
High	58
Critical	15



2.2 Hosts with Most Vulnerabilities

Presents the hosts with the most number of critical and high vulnerabilities. Hosts are ordered by the sum of critical and high vulnerabilities.

Host	FQDN	Critical Vulns	High Vulns
192.168.x.x		1	3
10.10.x.x		0	4
10.10.x.x		1	3
192.168.x.x		1	2
192.168.x.x		1	2
192.168.x.x		1	2
192.168.x.x		0	3
192.168.x.x		1	2
192.168.x.x		0	2
192.168.x.x		1	1

2.3 Most Common Vulnerabilities

Presents the 10 most common vulnerabilities of critical or high severity.

Name	Solution	Severity	Count
SSL Version 2 and 3 Protocol Detection	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	High	44
SNMP Agent Default Community Name (public)	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.	High	13
Microsoft SQL Server Unsupported Version Detection (remote check)	Upgrade to a version of Microsoft SQL Server that is currently supported.	Critical	6
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Upgrade to Dropbear SSH version 2016.74 or later.	Critical	6
nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities	Upgrade to nginx version 1.16.1 / 1.17.3 or later.	High	4
IPMI v2.0 Password Hash Disclosure	There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.	High	4
Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities	Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later.	High	2
Microsoft Windows SMB Shares	To restrict access under Windows, open Explorer, do a right click on each share, go to	High	2

Unprivileged Access	the 'sharing' tab, and click on 'permissions'.		
Telnetd - Remote Code Execution (CVE-2020-10188)	Refer to your vendor advisory regarding this issue.	Critical	1
VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0010)	Upgrade to VMware vCenter Server 6.5 U3p, 6.7 U3n, 7.0 U2b or later or apply the workaround mentioned in the advisory.	Critical	1

2.4 Most Common Remediations

Presents the 10 most common remediations for vulnerabilities of critical or high severity.

Service	Solution	Severity	Count
mssql	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	High	44
snmp	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.	High	13
mssql	Upgrade to a version of Microsoft SQL Server that is currently supported.	Critical	6
ssh	Upgrade to Dropbear SSH version 2016.74 or later.	Critical	6
www	Upgrade to nginx version 1.16.1 / 1.17.3 or later.	High	4
asf-rmcp	There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.	High	4
www	Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later.	High	2
cifs	To restrict access under Windows, open Explorer, do a right click on	High	2

	each share, go to the 'sharing' tab, and click on 'permissions'.		
telnet	Refer to your vendor advisory regarding this issue.	Critical	1
www	Upgrade to VMware vCenter Server 6.5 U3p, 6.7 U3n, 7.0 U2b or later or apply the workaround mentioned in the advisory.	Critical	1

2.5 Hosts with Exploitable Vulnerabilities

Presents the 10 most common remediations for vulnerabilities of critical or high severity.

Host	FQDN	Exploitable Critical Vulns	Exploitable High Vulns
192.168.x.x		1	2
192.168.x.x		0	1
192.168.x.x		0	1
192.168.x.x		1	0
192.168.x.x		0	1
192.168.x.x		0	1
192.168.x.x		0	1
192.168.x.x		0	1
192.168.x.x		0	0
192.168.x.x		0	0

2.6 Top Operating Systems

Displays the 10 most common operating systems identified.

OperatingSystem	Count
Linux Kernel 2.6	54
Windows	38
Windows Server 2016 Standard 14393	17
Linux Kernel 2.2 **Linux Kernel 2.4** **Linux Kernel 2.6**	14
Microsoft Windows Server 2012 R2 Standard	11
Microsoft Windows	8
SonicWALL	7
HP Switch	7
FortiOS on Fortinet FortiGate	6
iPhone or iPad	5

3 Recommendations

The highest number of vulnerabilities found in the assessment were related to Encryption. We realized a high number of affected hosts where the SSL certificate is not trusted, or where an old version of TLS encryption is used.

We would strongly recommend to update some applications on a regular basis. Especially the VMware vCenters should be kept a closer eye on, as the current installed versions are having several Vulnerabilities. Other Applications / Services should be updated regularly – for example the webservers using apache / tomcat, where nginx also had a remote code execution vulnerability. Dropbear SSH, or also an unsupported MS SQL version was detected in the assessment.

One vulnerability was detected on one Host which could also be used for Remote Code Execution (CVE-2020-10188) via Telnetd.

In the following list you find the Synopsis and its recommendations incl. their number of appearances. For further details please refer to the detailed report per network segment.

Synopsis	Remediation	Number of Hosts
The SSL certificate for this service cannot be trusted.	Purchase or generate a proper SSL certificate for this service.	145
The remote service encrypts traffic using an older version of TLS.	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	125
The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	Purchase or generate a proper SSL certificate for this service.	111
The remote service supports the use of medium strength SSL ciphers.	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	88
Signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	66
An SSL certificate in the certificate chain has been signed using a weak hash algorithm.	Contact the Certificate Authority to have the SSL certificate reissued.	65
The remote service supports the use of the RC4 cipher.	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	59
The SSL certificate for this service is for a different host.	Purchase or generate a proper SSL certificate for this service.	59

The remote SSH server is configured to allow weak key exchange algorithms.	Contact the vendor or consult product documentation to disable the weak algorithms.	43
The SSH server is configured to use Cipher Block Chaining.	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.	39
The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.	34
The remote service encrypts traffic using a protocol with known weaknesses.	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.	33
The remote server's SSL certificate has already expired.	Purchase or generate a new SSL certificate to replace the existing one.	32
The remote Terminal Services doesn't use Network Level Authentication only.	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.	31
It was possible to obtain sensitive information from the remote host with TLS-enabled services.	Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.	30
The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.	Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.	30
It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.	29
The remote web server is affected by multiple cross site scripting vulnerability.	Upgrade to JQuery version 3.5.0 or later.	19
The remote service supports the use of weak SSL ciphers.	Reconfigure the affected application, if possible to avoid the use of weak ciphers.	19
The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.	OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.	16
The remote Telnet server transmits traffic in cleartext.	Disable the Telnet service and use SSH instead.	15
The community name of the remote SNMP server can be guessed.	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.	13
It is possible to obtain information about the remote host.	Filter incoming traffic to UDP port 5353, if desired.	12

It may be possible to get access to the remote host.	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	10
The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.	Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.	8
The remote NTP server responds to mode 6 queries.	Restrict NTP mode 6 queries.	8
The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.	7
The remote host is not FIPS-140 compliant.	Change RDP encryption level to : 4. FIPS Compliant	7
An unsupported version of a database server is running on the remote host.	Upgrade to a version of Microsoft SQL Server that is currently supported.	6
The remote host is using weak cryptography.	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	6
The SSH service running on the remote host is affected by multiple vulnerabilities.	Upgrade to Dropbear SSH version 2016.74 or later.	6
Debugging functions are enabled on the remote web server.	Disable these HTTP methods. Refer to the plugin output for more information.	5
The remote host supports IPMI version 2.0.	There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.	4
The remote web server is affected by a remote code execution vulnerability.	Upgrade to nginx 1.20.1 or later.	3
The remote web server is affected by an information disclosure vulnerability.	Upgrade to nginx version 1.17.7 or later.	3
The remote web server is affected by multiple denial of service vulnerabilities.	Upgrade to nginx version 1.16.1 / 1.17.3 or later.	3

The remote web server contains default files.	Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.	3
The remote NTP server is affected by a denial of service vulnerability.	Upgrade to NTP version 4.2.8p9 or later.	3
The web application running on the remote web server is affected by a SSRF vulnerability.	Refer to vendor advisory.	2
The remote Apache Tomcat server is affected by a open redirect vulnerability.	Upgrade to Apache Tomcat version 8.5.34 or later.	2
The remote Apache Tomcat server is affected by a denial-of-service vulnerability	Upgrade to Apache Tomcat version 8.5.41 or later.	2
The remote Apache Tomcat server is affected by a vulnerability	Upgrade to Apache Tomcat version 8.5.49 or later.	2
The remote Apache Tomcat server is affected by a privilege escalation vulnerability	Upgrade to Apache Tomcat version 8.5.50 or later.	2
The remote Apache Tomcat server is affected by a remote code execution vulnerability	Upgrade to Apache Tomcat version 8.5.55 or later.	2
The remote Apache Tomcat server is affected by a denial of service vulnerability.	Upgrade to Apache Tomcat version 8.5.56 or later.	2
The remote Apache Tomcat server is affected by multiple vulnerabilities	Upgrade to Apache Tomcat version 8.5.57 or later.	2
The remote Apache Tomcat server is affected by an information disclosure vulnerability.	Upgrade to Apache Tomcat version 8.5.60 or later.	2
The remote Apache Tomcat server is affected by multiple vulnerabilities	Upgrade to Apache Tomcat version 8.5.63 or later.	2
The remote Apache Tomcat server is affected by a vulnerability	Upgrade to Apache Tomcat version 8.5.68 or later.	2
The remote Apache Tomcat server is affected by multiple vulnerabilities.	Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later.	2
The remote Apache Tomcat server is affected by a vulnerability	Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later.	2
The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.	Contact the vendor or consult product documentation to remove the weak ciphers.	2
The remote service supports the use of anonymous SSL ciphers.	Reconfigure the affected application if possible, to avoid use of weak ciphers.	2
It is possible to access a network share.	To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.	2
This web server leaks a private IP address through its HTTP headers.	Apply configuration suggested by vendor.	1

The remote web server is affected by a data disclosure vulnerability.	Either apply the patch manually or upgrade to nginx 1.12.1 / 1.13.3 or later.	1
The remote web server is affected by multiple vulnerabilities.	Upgrade to nginx 1.14.1 / 1.15.6 or later.	1
It is possible to get the list of files present in the remote directory.	- Configure your web server so as to prevent the download of .DS_Store files - Mac OS X users should configure their workstation to disable the creation of .DS_Store files on network shares.	1
The remote host supports a set of weak ciphers.	Reconfigure the service to remove support for EXPORT_RSA cipher suites.	1
The remote telnetd service is affected by a buffer overflow vulnerability that could lead to remote code execution.	Refer to your vendor advisory regarding this issue.	1
A network service running on the remote host is affected by multiple remote code execution vulnerabilities.	Upgrade to libupnp version 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.	1
The remote server is affected by multiple vulnerabilities.	Upgrade to Acme thttpd version 2.26 or later.	1
Tenable Nessus running on the remote host is affected by multiple vulnerabilities.	Upgrade to Tenable Nessus version 8.15.0 or later.	1
The remote SSH service is affected by multiple vulnerabilities.	Upgrade to the Dropbear SSH 2013.59 or later.	1
A Redis server is not protected by password authentication.	Enable the 'requirepass' directive in the redis.conf configuration file.	1
The remote host supports a set of weak ciphers.	Reconfigure the service to remove support for EXPORT_DHE cipher suites.	1
A licensing application running on the remote host is affected by multiple vulnerabilities.	Upgrade to FlexNet Publisher 11.16.2 or later.	1
The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.	Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.	1
A virtualization management application installed on the remote host is affected by a arbitrary file upload vulnerability.	Upgrade to VMware vCenter Server 7.0 U2c or later or apply the workaround mentioned in the advisory.	1
A virtualization management application installed on the remote host is affected by multiple vulnerabilities.	Upgrade to VMware vCenter Server 7.0 U2d or later or apply the workaround mentioned in the advisory.	1
A virtualization management application installed on the remote host is affected by multiple vulnerabilities.	Upgrade to VMware vCenter Server 7.0 U2c or later or apply the workaround mentioned in the advisory.	1
A virtualization management application installed on the remote	Upgrade to VMware vCenter Server 6.5 U3p, 6.7 U3n, 7.0 U2b or later or apply the workaround mentioned in the advisory.	1

host is affected by multiple vulnerabilities.		
At least one iSCSI target is configured not to use authentication.	Configure authentication on the target to restrict access to authorized initiators.	1