NAME :- M Om Nivas REG no :- 21BCE9706

Email :- omnivas.21bce9706@vitapstudent.ac.in

Task – 8

Nessus Scanning Report :-

Vulnerability Name :-

SSH Weak Key Exchange Algorithms Enabled

CWE (Common weakness enumeration) :-

CWE-326: Inadequate Encryption Strength

OWASP (open worldwide application security project) :-

Use Strong Encryption Algorithms:

Secure Key Management:

Secure Transport Layer:

Data Classification:

Secure Defaults:

Third-Party Libraries:

Description :-

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled.

This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Business Impact :-

Data Breaches and Unauthorized Access

Loss of Confidential Information

Financial Loss

Operational Disruption

Reputation Damage

Regulatory Non-Compliance

Loss of Competitive Advantage

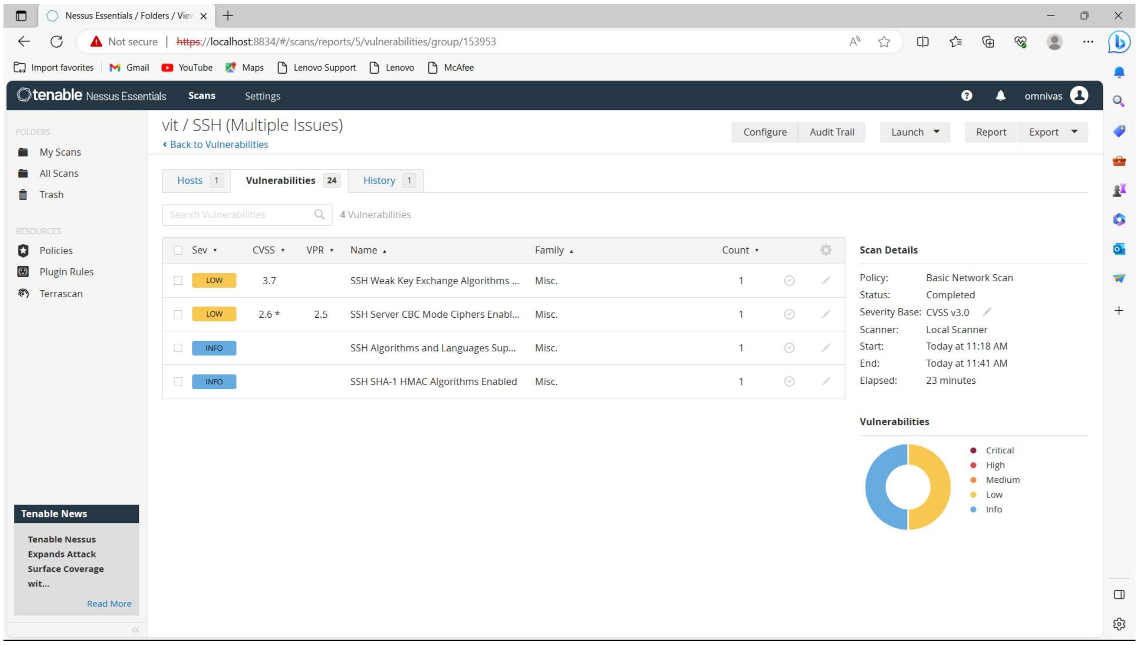
Long-Term Repercussions

Resource Drain

Customer and Employee Trust

Affected URL :- https://vitap.ac.in/

POC (Proof of Concept) :-



vit / SSH (Multiple Issues)

‹ Back to Vulnerabilities

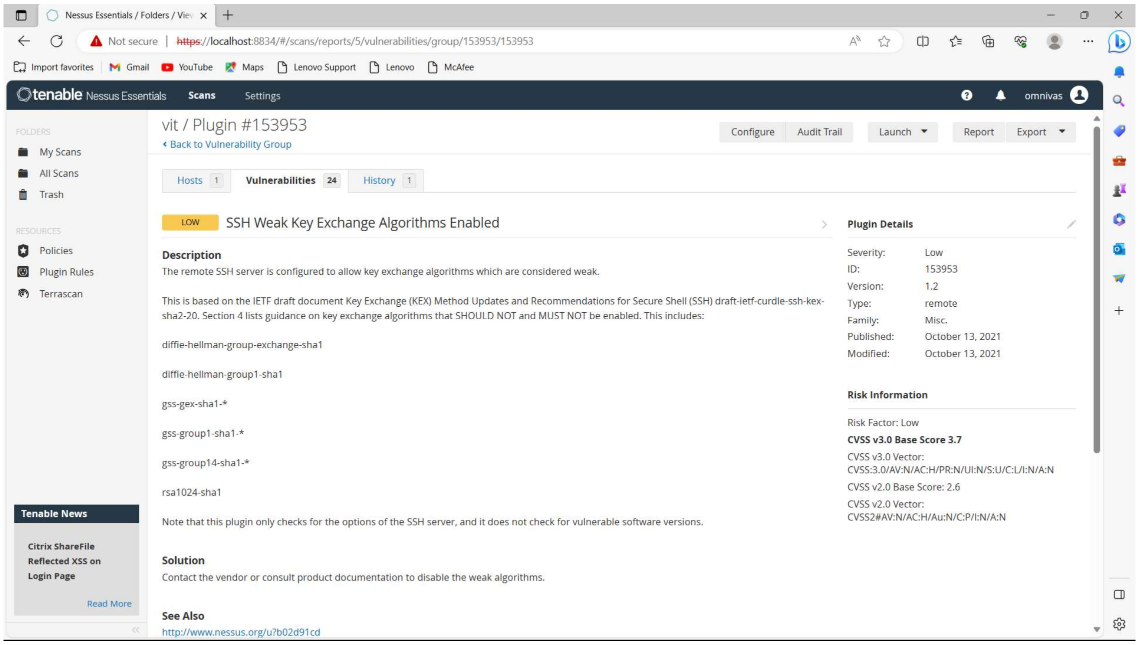
4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
LOW	3.7		SSH Weak Key Exchange Algorithms ...	Misc.	1
LOW	2.6 *	2.5	SSH Server CBC Mode Ciphers Enabl...	Misc.	1
INFO			SSH Algorithms and Languages Sup...	Misc.	1
INFO			SSH SHA-1 HMAC Algorithms Enabled	Misc.	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:18 AM
End:	Today at 11:41 AM
Elapsed:	23 minutes

Vulnerabilities



vit / Plugin #153953

‹ Back to Vulnerability Group

LOW SSH Weak Key Exchange Algorithms Enabled

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

See Also

http://www.nessus.org/u?b02d91cd

Plugin Details

Severity:	Low
ID:	153953
Version:	1.2
Type:	remote
Family:	Misc.
Published:	October 13, 2021
Modified:	October 13, 2021

Risk Information

Risk Factor: Low

CVSS v3.0 Base Score 3.7

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Base Score: 2.6

CVSS v2.0 Vector:
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Remediation :-

Identify Weak Algorithms

Update SSH Software

Configuration Settings

Preferred Algorithms

Key Lengths

Host Key Algorithms

Testing and Validation

Logging and Monitoring

Documentation and Training

Regular Updates

Compliance Checks

Consider SSH Hardening Guides