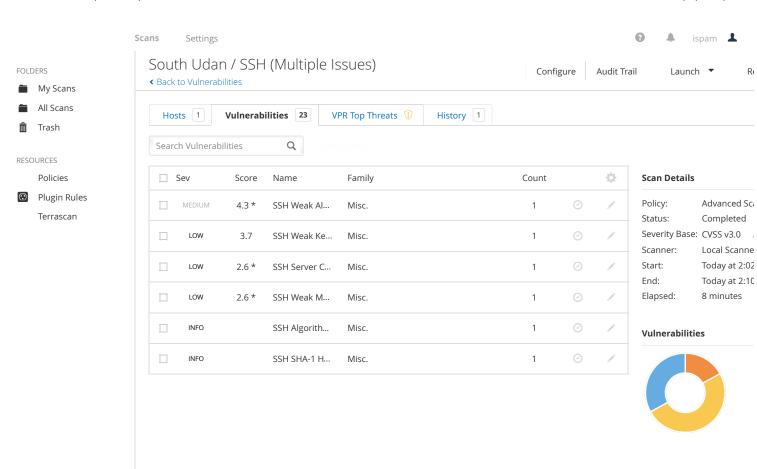


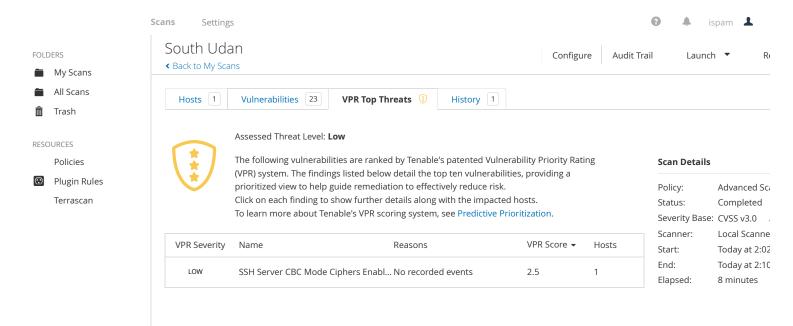
https://127.0.0.1:8834/#/scans/reports/17/vulnerabilities

<<



CVE-2022-27510:
Critical Citrix ADC
and Gateway Au...

Read More



Tenable News

Microsoft's November 2022 Patch Tuesday Addresses ...

Read More

<<

LOW SSH Server CBC Mode Ciphers Enabled

×

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Vulnerability Priority Rating

Age of vuln: 730 days + CVSSv3 Impact Score: 2.5 Exploit Code Maturity: Unproven Product Coverage: High

Threat Intensity: Very Low

Threat Recency: No recorded events

Threat Sources: No recorded events

Affected Hosts (1)

192.168.56.102

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

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

Solution

 $Contact \ the \ vendor \ or \ consult \ product \ documentation \ to \ disable \ CBC \ mode \ cipher \ encryption, \ and \ enable \ CTR \ or \ GCM \ cipher \ mode \ encryption.$