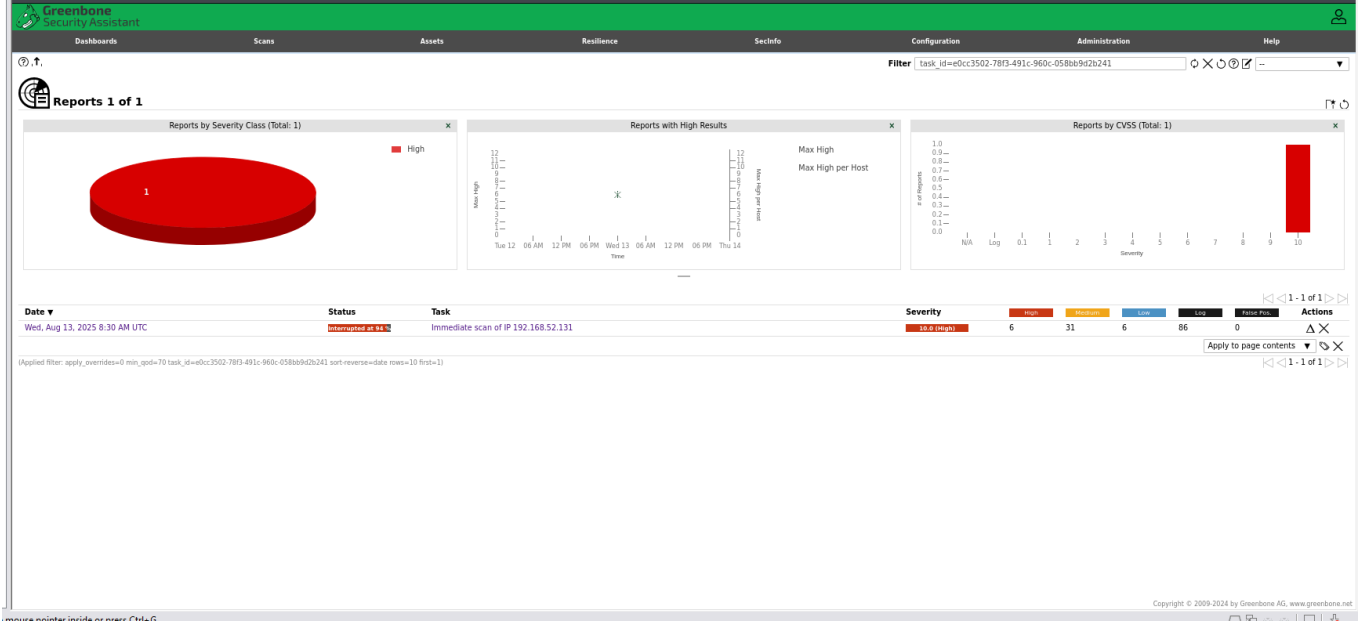
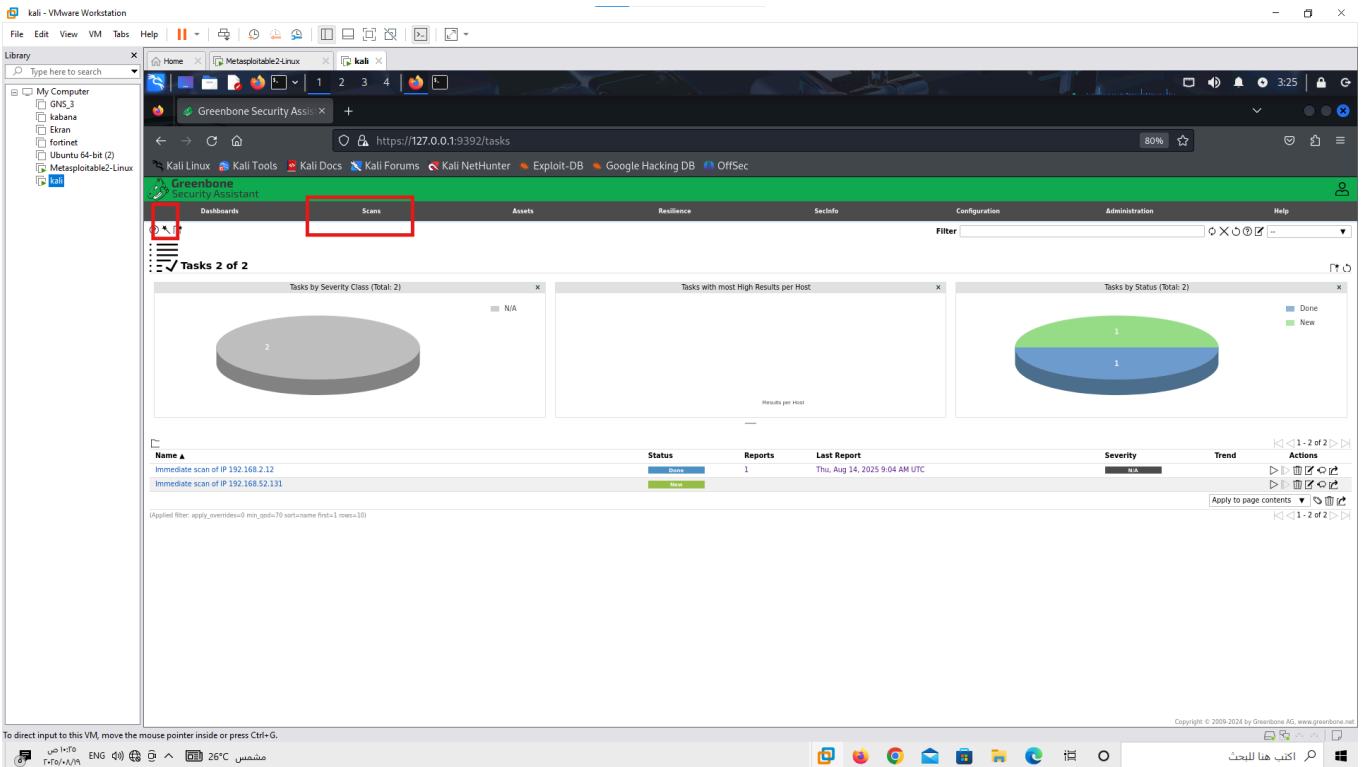


هنا استخدمنا اداة (OpenVAS) وهي تعمل على تحليل الانظمة للتعرف على انواع الثغرات والتهديدات الموجودة على النظام والبروتات المفتوحة ومالي ذلك.

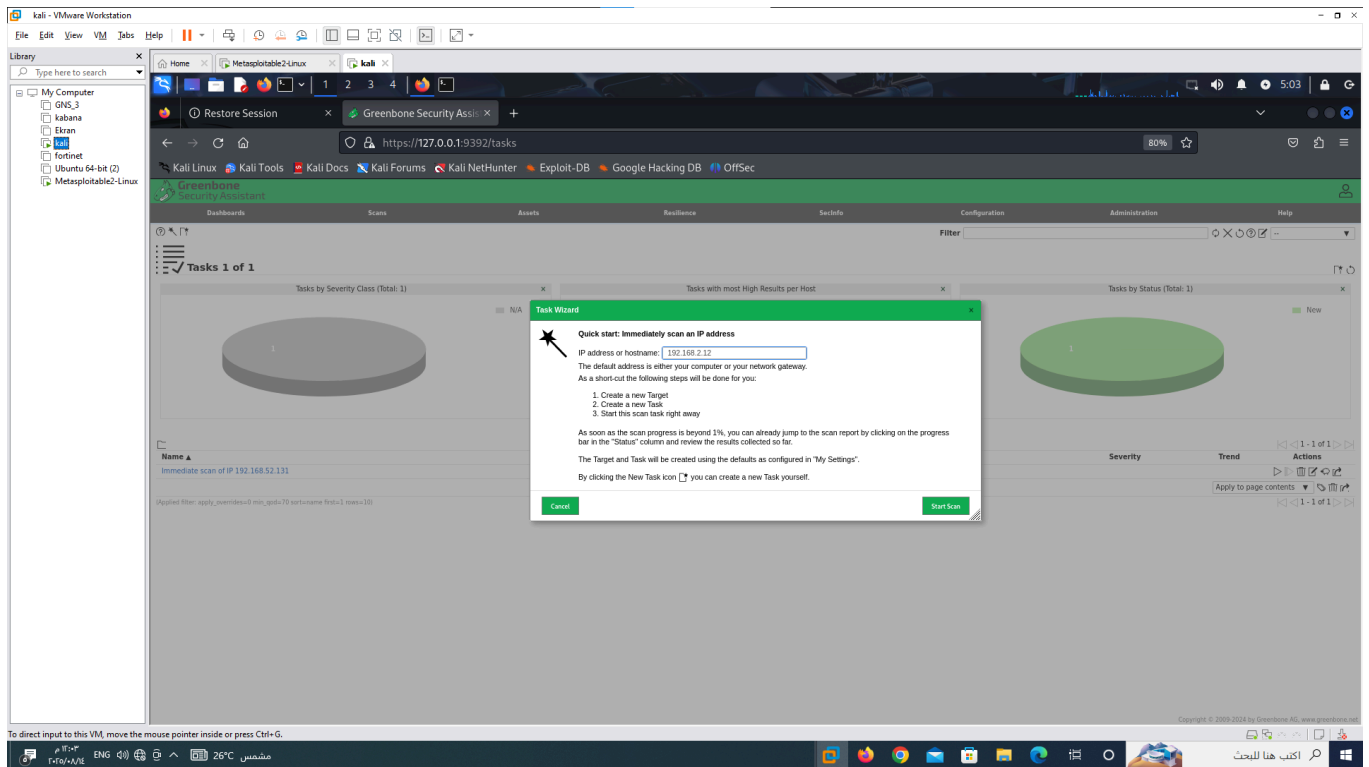
1-الطريقة الاولى:الدخول للاداة عبر المتصفح عبر البورت (9392 localhost).  
هذه الواجهة الرئيسية ال (dashboards)للاداة



2-الطريقة الثانية :انشئ مهمة جديدة من خلال الضغط على (scan) ثم الضغط على السهم المشار اليه

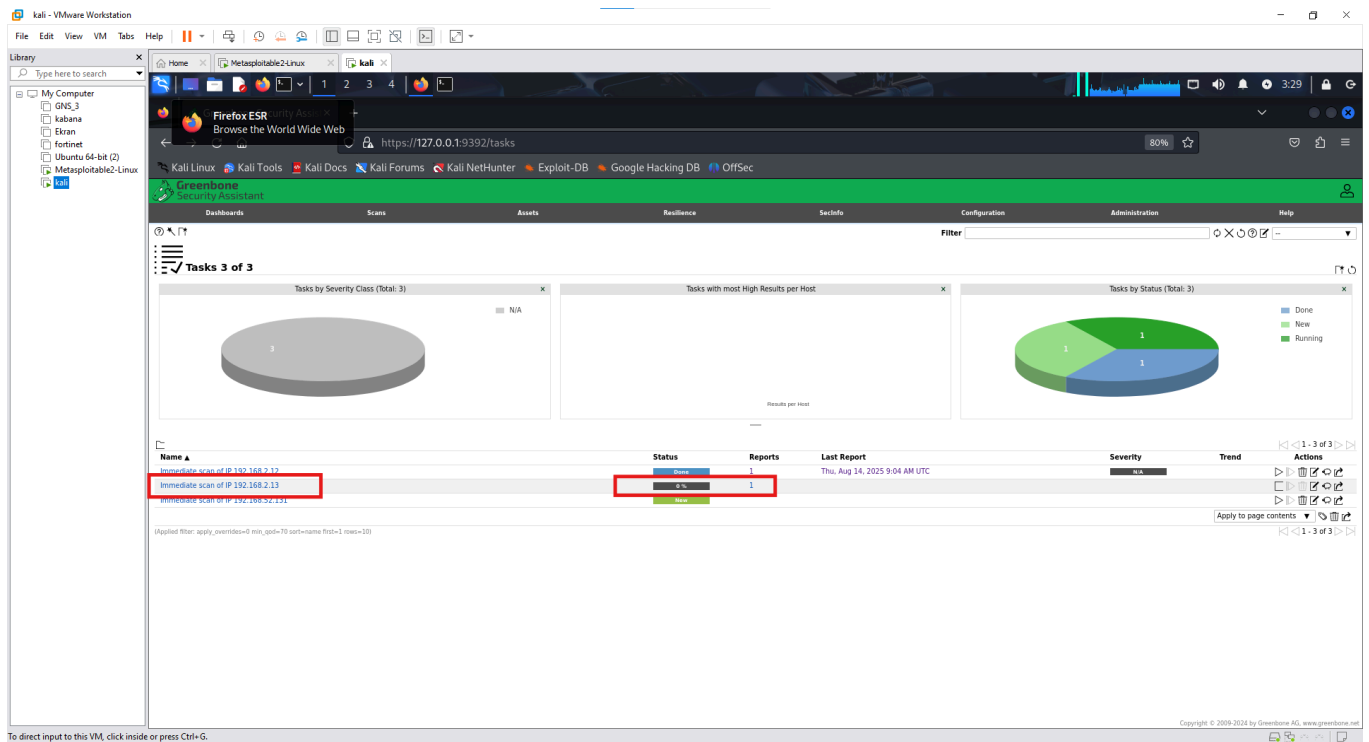


3-الطريقة الثالثة:  
ادخل العنوان تبع الظام الذي تريد فحصة



#### 4-الطريقة الرابعة:

هنا يظهر عنوان النظام الذي قمنا بتحديد ومقابلة عداد الفحص المشار اليه بالصورة ادناه



#### 5-الطريقة الخامسة:

هذه نتائج الفحص من ثغرات ومن بورتات وانواع اخرى تدل على تهديدات في النظام

kali - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- GNS\_3
- kabana
- Ekan
- fortinet
- Ubuntu 64-bit (2)
- Metasploitable2-Linux

Greenbone Security Assistant

https://127.0.0.1:9392/report/122512e1-4b92-41db-9ac5-8e3bd6b97433

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Tue, Aug 19, 2025 7:28 AM UTC 94 %

ID: 122512e1-4b92-41db-9ac5-8e3bd6b97433 Created: Tue, Aug 19, 2025 7:28 AM UTC Modified: Tue, Aug 19, 2025 7:49 AM UTC Owner: admin

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

(57 of 592) (1 of 1) (18 of 23) (0 of 0) (0 of 0) (26 of 26) (0 of 0) (2 of 2) (0 of 0) (0)

Vulnerability Severity QoD Host Name Location Created

rlogin Passwordless Login	10.0 (High)	80 %	192.168.2.13		513/tcp	Tue, Aug 19, 2025 7:42 AM UTC
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	192.168.2.13		8787/tcp	Tue, Aug 19, 2025 7:48 AM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.2.13		general/tcp	Tue, Aug 19, 2025 7:43 AM UTC
Possible Backdoor: Ingresslock	10.0 (High)	99 %	192.168.2.13		1524/tcp	Tue, Aug 19, 2025 7:49 AM UTC
The rexec service is running	10.0 (High)	80 %	192.168.2.13		512/tcp	Tue, Aug 19, 2025 7:44 AM UTC
Twiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.2.13		80/tcp	Tue, Aug 19, 2025 7:45 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	9.8 (High)	99 %	192.168.2.13		21/tcp	Tue, Aug 19, 2025 7:48 AM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	9.8 (High)	95 %	192.168.2.13		3306/tcp	Tue, Aug 19, 2025 7:47 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	9.8 (High)	99 %	192.168.2.13		6200/tcp	Tue, Aug 19, 2025 7:48 AM UTC
DisCC RCE Vulnerability (CVE-2004-2687)	9.8 (High)	99 %	192.168.2.13		3632/tcp	Tue, Aug 19, 2025 7:48 AM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	9.8 (High)	99 %	192.168.2.13		5432/tcp	Tue, Aug 19, 2025 7:47 AM UTC
VNC Brute Force Login	9.8 (High)	95 %	192.168.2.13		5900/tcp	Tue, Aug 19, 2025 7:45 AM UTC
Ricello NetMan 204 Default Credentials (SSH)	7.5 (High)	100 %	192.168.2.13		22/tcp	Tue, Aug 19, 2025 7:47 AM UTC
Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	7.5 (High)	95 %	192.168.2.13		1099/tcp	Tue, Aug 19, 2025 7:48 AM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	192.168.2.13		514/tcp	Tue, Aug 19, 2025 7:44 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.2.13		21/tcp	Tue, Aug 19, 2025 7:47 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.2.13		2121/tcp	Tue, Aug 19, 2025 7:47 AM UTC
The rlogin service is running	7.5 (High)	80 %	192.168.2.13		513/tcp	Tue, Aug 19, 2025 7:44 AM UTC
Twiki Cross-Site Request Forgery Vulnerability (Sep 2010)	6.8 (Medium)	80 %	192.168.2.13		80/tcp	Tue, Aug 19, 2025 7:45 AM UTC
Anonymous FTP Login Reporting	6.8 (Medium)	80 %	192.168.2.13		21/tcp	Tue, Aug 19, 2025 7:42 AM UTC
Twiki < 6.1.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.2.13		80/tcp	Tue, Aug 19, 2025 7:45 AM UTC

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Copyright © 2000-2024 by Greenbone AG, www.greenbone.net

kali - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- GNS\_3
- kabana
- Ekan
- fortinet
- Ubuntu 64-bit (2)
- Metasploitable2-Linux

Greenbone Security Assistant

https://127.0.0.1:9392/report/122512e1-4b92-41db-9ac5-8e3bd6b97433

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Tue, Aug 19, 2025 7:28 AM UTC 96 %

ID: 122512e1-4b92-41db-9ac5-8e3bd6b97433 Created: Tue, Aug 19, 2025 7:28 AM UTC Modified: Tue, Aug 19, 2025 7:52 AM UTC Owner: admin

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

(64 of 599) (1 of 1) (19 of 23) (0 of 0) (0 of 0) (31 of 31) (0 of 0) (2 of 2) (0 of 0) (0)

Port Hosts Severity

80/tcp	1	10.0 (High)
512/tcp	1	10.0 (High)
513/tcp	1	10.0 (High)
1524/tcp	1	10.0 (High)
8787/tcp	1	10.0 (High)
21/tcp	1	9.8 (High)
22/tcp	1	9.8 (High)
3306/tcp	1	9.8 (High)
6200/tcp	1	9.8 (High)
8009/tcp	1	9.8 (High)
3632/tcp	1	9.8 (High)
5432/tcp	1	9.8 (High)
5900/tcp	1	9.8 (High)
514/tcp	1	7.5 (High)
1099/tcp	1	7.5 (High)
2121/tcp	1	7.5 (High)
25/tcp	1	6.8 (Medium)
445/tcp	1	6.8 (Medium)
23/tcp	1	4.4 (Medium)

Applied filter: apply\_overview=0 levels=html rows=100 min\_qods=70 find=1 sort=severity=severity

Copyright © 2000-2024 by Greenbone AG, www.greenbone.net

kali - VMware Workstation

Library

Home | Metasploitable2-Linux | kali

Greenbone Security Assistant

Report: Tue, Aug 19, 2025 7:28 AM UTC

Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags

CVE-1999-0618 NVT The rexec service is running Hosts 1 Occurrences 1 Severity 10.0 (High)

CVE-2008-5304 CVE-2008-5305 TWiki XSS and Command Execution Vulnerabilities 1 1 10.0 (High)

CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2020-29583 CVE-2020-9473 CVE-2023-1944 CVE-2024-22902 CVE-2024-31970 CVE-2024-46328 SSH Brute Force Logins With Default Credentials Reporting 1 1 9.8 (High)

CVE-2001-0845 CVE-2002-1809 CVE-2004-1530 CVE-2004-2257 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719 CVE-2024-22901 MySQL / MariaDB Default Credentials (MySQL Protocol) 1 1 9.8 (High)

CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335 PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check 1 1 9.8 (High)

CVE-2011-2523 vsftpd Compromised Source Packages Backdoor Vulnerability 1 2 9.8 (High)

CVE-2020-1938 Apache Tomcat AJP RCE Vulnerability (Ghostcat) 1 1 9.8 (High)

CVE-2004-2687 DistCC RCE Vulnerability (CVE-2004-2687) 1 1 9.8 (High)

CVE-1999-0651 rsh Unencrypted Cleartext Login 1 1 7.5 (High)

CVE-2011-3556 Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check 1 1 7.5 (High)

CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2014-9198 CVE-2015-7261 CVE-2016-8731 CVE-2017-6218 CVE-2018-9068 CVE-2018-17771 CVE-2018-19063 CVE-2018-19064 FTP Brute Force Logins Reporting 1 2 7.5 (High)

CVE-1999-0651 The rlogin service is running 1 1 7.5 (High)

CVE-2014-0224 SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability 1 1 7.4 (High)

CVE-2009-4898 TWiki Cross-Site Request Forgery Vulnerability (Sep 2010) 1 1 6.8 (Medium)

CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165 Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V... 1 1 6.8 (Medium)

CVE-1999-0497 Anonymous FTP Login Reporting 1 1 6.4 (Medium)

CVE-2012-6708 jQuery < 1.9.0 XSS Vulnerability 1 1 6.3 (Medium)

CVE-2018-20212 TWiki < 6.1.0 XSS Vulnerability 1 1 6.3 (Medium)

CVE-2007-2447 Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check 1 1 6.0 (Medium)

CVE-2009-1339 TWiki CSRF Vulnerability 1 1 6.0 (Medium)

CVE-2016-0800 CVE-2014-3566 SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection 1 2 5.9 (Medium)

CVE-2013-2566 CVE-2015-2808 CVE-2015-4000 SSL/TLS: Report Weak Cipher Suites 1 1 5.9 (Medium)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

هذه تفاصيل حول ثغرة معينة من الثغرات الموجودة على النظام

kali - VMware Workstation

Library

Home | Metasploitable2-Linux | kali

Greenbone Security Assistant

CVE: CVE-2024-46328

Information User Tags

Description

VONETS VAP11G-300 v3.3.23.6.9 was discovered to contain hardcoded credentials for several different privileged accounts, including root.

CVSS

Base Score 8.0 (High)

Base Vector CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Attack Vector Adjacent

Attack Complexity Low

Privileges Required None

User Interaction None

Scope Unchanged

Confidentiality Impact High

Integrity Impact High

Availability Impact High

References

<https://hackerone.com/55196444-2466-4924-b7c8-8f07742117be/9461d352-c4f6-477f-a44e-b91f71e6d84.pdf>

NVTs addressing this CVE

HTTP Brute Force Logins With Default Credentials Reporting

SSH Brute Force Logins With Default Credentials Reporting

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

