GROUP 8

Dec 03, 2023

PROJECT –TVRA REPORT

ISMAIL MAHAMED 125052191

JASKARAN SOHAL 150343218

RAYYAN KHAN 155534209

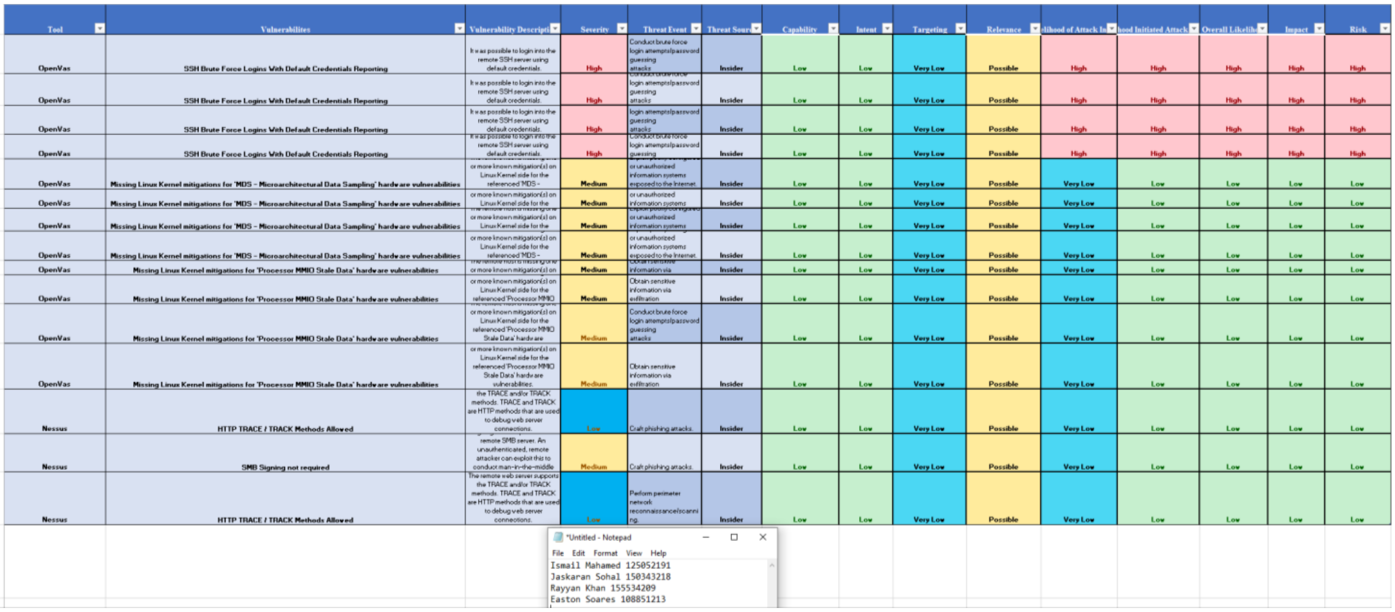
EASTON SOARES 108851213

Table of Contents

TVRA Report

Introduction

Our network infrastructure is diligently segmented into zones that facilitate administrative efficiency, external web interaction, and overarching network management. In the face of persistent cyber threats, we continuously evaluate these zones to fortify our defenses. A prevalent concern is the vulnerability to SSH brute force attacks, a common yet critical security challenge that could compromise our network through widely utilized ports. The implications of such breaches are far-reaching, potentially causing operational interruptions, financial detriment, and reputational damage. This underscores the imperative for stringent security measures.



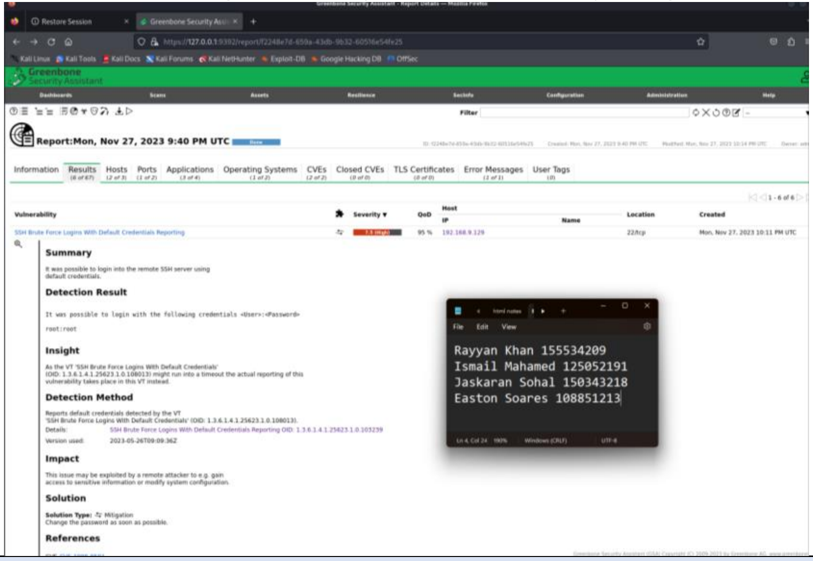
Tool	Vulnerabilites	Vulnerability Descripti	Severity	Threat Event	Threat Sour	Capability	Intent	Targeting	Relevance	elihood of Attack In	hood Initiated Attack	Overall Likelih	Impact	Risk
OpenVas	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.	High	Conduct brute force login attempts/password guessing attacks	Insider	Low	Low	Very Low	Possible	High	High	High	High	High
OpenVas	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.	High	login attempts/password guessing attacks	Insider	Low	Low	Very Low	Possible	High	High	High	High	High
OpenVas	SSH Brute Force Logins With Default Credentials Reporting	It was possible to login into the remote SSH server using default credentials.	High	login attempts/password guessing attacks	Insider	Low	Low	Very Low	Possible	High	High	High	High	High
OpenVas	SSH Brute Force Logins With Default Credentials Reporting	remote SSH server using default credentials.	High	login attempts/password guessing	Insider	Low	Low	Very Low	Possible	High	High	High	High	High
OpenVas	Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the referenced 'MDS –	Medium	or unauthorized information systems exposed to the Internet.	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the	Medium	or unauthorized information systems	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the	Medium	or unauthorized information systems	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the referenced 'MDS –	Medium	or unauthorized information systems exposed to the Internet.	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	or more known mitigation(s) on	Medium	information via	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO	Medium	Obtain sensitive information via exfiltration	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware	Medium	Conduct brute force login attempts/password guessing attacks	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
OpenVas	Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities.	Medium	Obtain sensitive information via exfiltration	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
Nessus	HTTP TRACE / TRACK Methods Allowed	the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.	Low	Craft phishing attacks.	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
Nessus	SMB Signing not required	remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle	Medium	Craft phishing attacks.	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low
Nessus	HTTP TRACE / TRACK Methods Allowed	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.	Low	Perform perimeter network reconnaissance/scanning.	Insider	Low	Low	Very Low	Possible	Very Low	Low	Low	Low	Low

```
Ismail Mahamed 125052191
Jaskaran Sohal 150343218
Rayyan Khan 155534209
Easton Soares 108851213
```

This TVRA delves into the SSH vulnerability, among others, assessing not only the technical risks but also the associated business impacts. Should such vulnerabilities be exploited, the resulting damage could span from tangible operational halts to intangible losses of stakeholder trust. Our comprehensive analysis is designed to steer the development of a robust mitigation strategy to bolster network resilience and ensure business continuity.

For a detailed account of our security posture, the vulnerabilities we face, and the strategies recommended to address these challenges, please refer to the full report below.

Vulnerabilities

Vulnerability	*SSH Brute Force Logins with Default Credentials Reporting* 
Vulnerability Description	It was possible to login into the remote SSH server using default credentials.
Vulnerability Severity	High
Level of Impact	High
Overall Likelihood	High
Risk	High
Business Impact	A successful attack could lead to operational disruptions and financial losses due to data breaches or system outages. Reputation damage and legal penalties due to non-compliance with regulations could also occur.
Mitigation	Implement strong, unique passwords, disable default accounts, and enforce account lockout policies. Regularly audit and monitor SSH logs.

Report:Mon, Nov 27, 2023 9:40 PM UTC

Information | Results (6 of 67) | Hosts (2 of 3) | Ports (1 of 2) | Applications (3 of 4) | Operating Systems (1 of 2) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (1 of 1) | User Tags (0)

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.9.129		22/tcp	Mon, Nov 27, 2023 10:11 PM UTC

Summary

It was possible to login into the remote SSH server using default credentials.

Detection Result

```
It was possible to login with the following credentials <User>:<Password>

root:root
```

Insight

As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Detection Method

Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).

Details: SSH Brute Force Logins With Default Credentials Reporting OID: 1.3.6.1.4.1.25623.1.0.103239

Version used: 2023-05-26T09:09:36Z

Impact

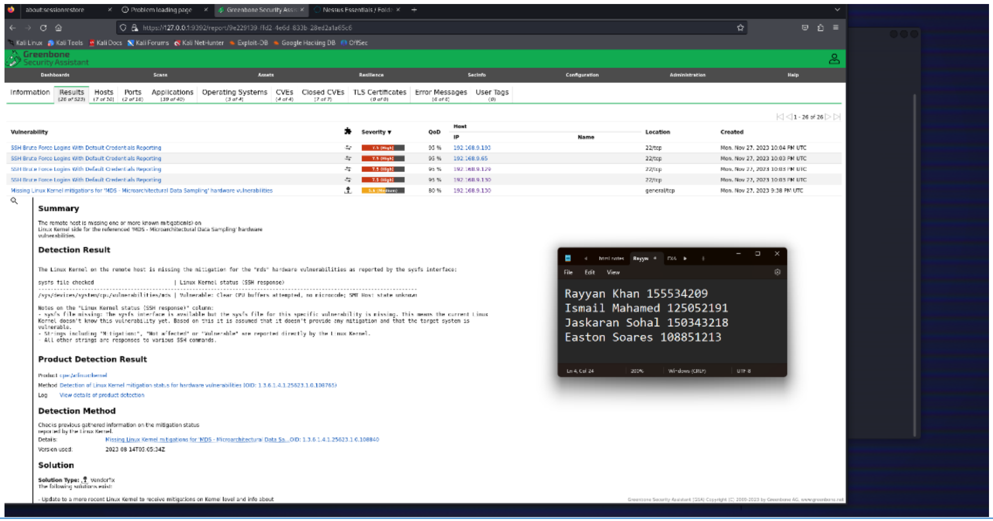
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution

Solution Type: Mitigation
Change the password as soon as possible.

References

```
Rayyan Khan 155534209
Ismail Mahamed 125052191
Jaskaran Sohal 150343218
Easton Soares 108851213
```

Vulnerability	Missing Linux Kernel mitigations for 'MDS- Microarchitectural Data Sampling' hardware vulnerabilities 

https://127.0.0.1:9392/report/9e229139-ffd2-4e6d-833b-28ed2a1a65c6

Information | Results (26 of 523) | Hosts (7 of 10) | Ports (2 of 18) | Applications (39 of 40) | Operating Systems (3 of 4) | CVEs (4 of 4) | Closed CVEs (7 of 7) | TLS Certificates (0 of 0) | Error Messages (4 of 4) | User Tags (0)

1 - 26 of 26

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.9.193		22/tcp	Mon, Nov 27, 2023 10:04 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.9.65		22/tcp	Mon, Nov 27, 2023 10:03 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.9.129		22/tcp	Mon, Nov 27, 2023 10:03 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.9.130		22/tcp	Mon, Nov 27, 2023 10:03 PM UTC
Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities	5.5 (Medium)	80 %	192.168.9.130		general/tcp	Mon, Nov 27, 2023 9:38 PM UTC

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities.

Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "mds" hardware vulnerabilities as reported by the sysfs interface:

sysfs file checked                        | Linux Kernel status (SSH response)
--------------------------------------------------------------------------------
/sys/devices/system/cpu/vulnerabilities/mds | Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown

Notes on the "Linux Kernel status (SSH response)" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for this specific vulnerability is missing. This means the current Linux
Kernel doesn't know this vulnerability yet. Based on this it is assumed that it doesn't provide any mitigation and that the target system is
vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported directly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Product Detection Result

Product cpe:/a:linux:kernel

Method Detection of Linux Kernel mitigation status for hardware vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.108765)

Log View details of product detection

Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.

Details: Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sa... OID: 1.3.6.1.4.1.25623.1.0.108840

Version used: 2023-08-14T05:05:34Z

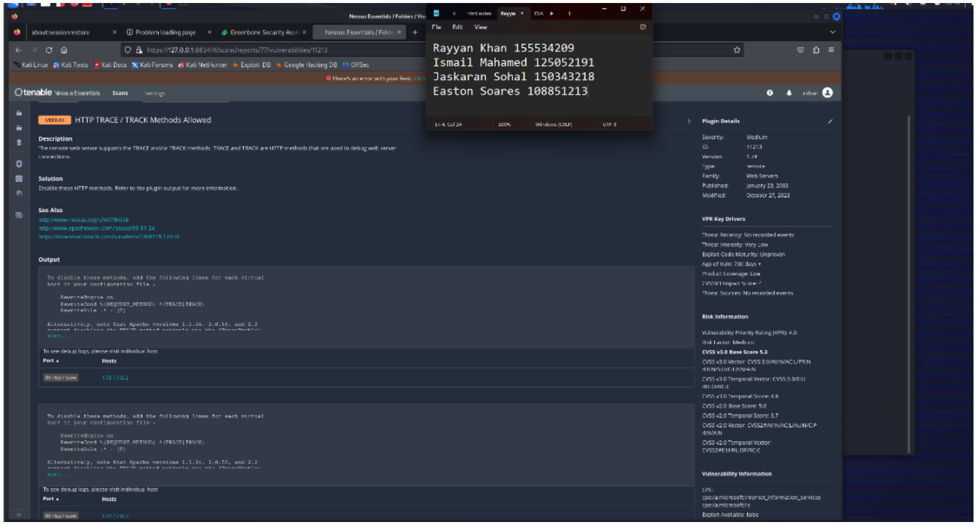
Solution

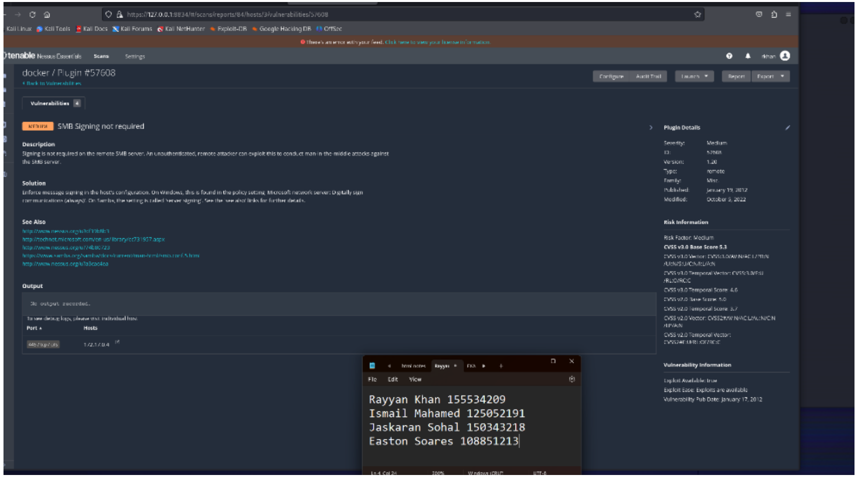
Solution Type: VendorFix
The following solutions exist:

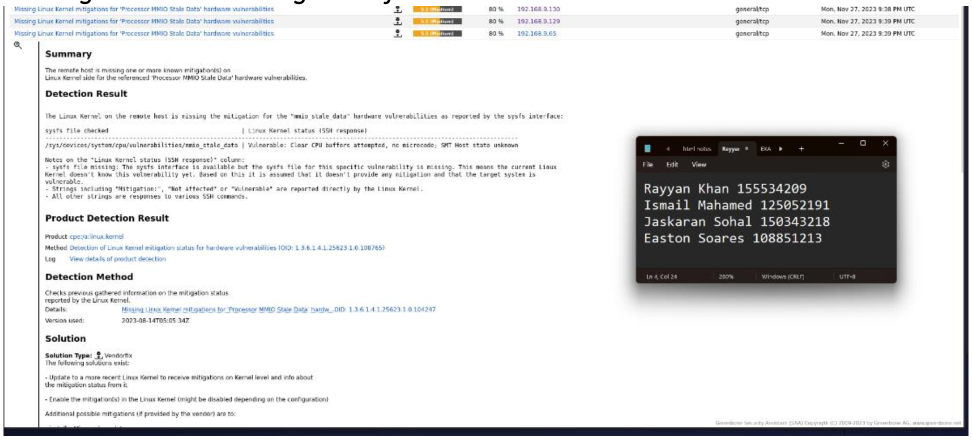
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about

```
Rayyan Khan 155534209
Ismail Mahamed 125052191
Jaskaran Sohal 150343218
Easton Soares 108851213
```

Vulnerability Description	The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities.
Vulnerability Severity	Medium
Level of Impact	Low
Overall Likelihood	Low
Risk	Low
Business Impact	Exposure of sensitive data could result in intellectual property theft, customer trust erosion, and legal ramifications.
Mitigation	Apply the latest kernel patches and updates and check for microcode updates from hardware vendors.

Vulnerability	***HTTP TRACE / TRACK Methods Allowed***  Nessus Essentials / Folders / Vie about:sessionrestore Problem loading page Greenbone Security Assis Nessus Essentials / Folde Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec html notes Rayya EXA File Edit View tenable Nessus Essentials Scans Settings rkhan https://127.0.0.1:8834/#/scans/reports/77/vulnerabilities/11213 Rayyan Khan 155534209 Ismail Mahamed 125052191 Jaskaran Sohal 150343218 Easton Soares 108851213 Ln 4, Col 24 200% Windows (CRLF) UTF-8 There's an error with your feed. MEDIUM HTTP TRACE / TRACK Methods Allowed **Description** The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. **Solution** Disable these HTTP methods. Refer to the plugin output for more information. **See Also** http://www.nessus.org/u?e979b5cb http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html **Output** To disable these methods, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 more... To see debug logs, please visit individual host Port ▲ Hosts 80 / tcp / www 172.17.0.2 To disable these methods, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 more... To see debug logs, please visit individual host Port ▲ Hosts 80 / tcp / www 172.17.0.3 **Plugin Details** Severity: Medium ID: 11213 Version: 1.74 Type: remote Family: Web Servers Published: January 23, 2003 Modified: October 27, 2023 **VPR Key Drivers** Threat Recency: No recorded events Threat Intensity: Very Low Exploit Code Maturity: Unproven Age of Vuln: 730 days + Product Coverage: Low CVSSV3 Impact Score: [illegible] Threat Sources: No recorded events **Risk Information** Vulnerability Priority Rating (VPR): 4.0 Risk Factor: Medium **CVSS v3.0 Base Score 5.3** CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C CVSS v3.0 Temporal Score: 4.6 CVSS v2.0 Base Score: 5.0 CVSS v2.0 Temporal Score: 3.7 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C **Vulnerability Information** CPE: cpe:/a:microsoft:internet_information_services cpe:/a:microsoft:iis Exploit Available: false
Vulnerability Description	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
Vulnerability Severity	Low
Level of Impact	Low
Overall Likelihood	Low
Risk	Low
Business Impact	Disclosure of internal network details could aid further attacks, leading to website compromise and undermining customer confidence in web services security.
Mitigation	Disable HTTP TRACE and TRACK methods on web servers and configure them to reject such requests.

Vulnerability	***SMB Signing not required.***  https://127.0.0.1:8834/#/scans/reports/84/hosts/3/vulnerabilities/57608 There's an error with your feed. Click here to view your license information. docker / Plugin #57608 Back to Vulnerabilities MEDIUM SMB Signing not required **Description** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. **Solution** 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. **See Also** http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea **Output** No output recorded. To see debug logs, please visit individual host. Port ▲ Hosts 445/tcp/cifs 172.17.0.4 **Plugin Details** Severity: Medium ID: 57608 Version: 1.20 Type: remote Family: Misc. Published: January 19, 2012 Modified: October 5, 2022 **Risk Information** Risk Factor: Medium **CVSS v3.0 Base Score 5.3** CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C CVSS v3.0 Temporal Score: 4.6 CVSS v2.0 Base Score: 5.0 CVSS v2.0 Temporal Score: 3.7 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C **Vulnerability Information** Exploit Available: true Exploit Ease: Exploits are available Vulnerability Pub Date: January 17, 2012 Rayyan Khan 155534209 Ismail Mahamed 125052191 Jaskaran Sohal 150343218 Easton Soares 108851213
Vulnerability Description	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
Vulnerability Severity	Medium
Level of Impact	Low
Overall Likelihood	Low
Risk	Low
Business Impact	Compromise of data integrity and potential operational sabotage could cause critical business processes to cease, incurring financial and operational losses.
Mitigation	Enforce SMB signing on all devices to ensure data integrity and prevent unauthorized access.

Vulnerability	***Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware***  Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities 5.5 (Medium) 80 % 192.168.9.130 general/tcp Mon, Nov 27, 2023 9:38 PM UTC Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities 5.5 (Medium) 80 % 192.168.9.129 general/tcp Mon, Nov 27, 2023 9:39 PM UTC Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities 5.5 (Medium) 80 % 192.168.9.65 general/tcp Mon, Nov 27, 2023 9:39 PM UTC **Summary** The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities. **Detection Result** The Linux Kernel on the remote host is missing the mitigation for the "mmio_stale_data" hardware vulnerabilities as reported by the sysfs interface: sysfs file checked | Linux Kernel status (SSH response) /sys/devices/system/cpu/vulnerabilities/mmio_stale_data | Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown Notes on the "Linux Kernel status (SSH response)" column: - sysfs file missing: The sysfs interface is available but the sysfs file for this specific vulnerability is missing. This means the current Linux Kernel doesn't know this vulnerability yet. Based on this it is assumed that it doesn't provide any mitigation and that the target system is vulnerable. - Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported directly by the Linux Kernel. - All other strings are responses to various SSH commands. **Product Detection Result** Product cpe:/a:linux:kernel Method Detection of Linux Kernel mitigation status for hardware vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.108765) Log View details of product detection **Detection Method** Checks previous gathered information on the mitigation status reported by the Linux Kernel. Details: Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardw...OID: 1.3.6.1.4.1.25623.1.0.104247 Version used: 2023-08-14T05:05:34Z **Solution** **Solution Type:** Vendorfix The following solutions exist: - Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it - Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration) Additional possible mitigations (if provided by the vendor) are to: Rayyan Khan 155534209 Ismail Mahamed 125052191 Jaskaran Sohal 150343218 Easton Soares 108851213
Vulnerability Description	is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities.
Vulnerability Severity	Medium

Level of Impact	Low
Overall Likelihood	Low
Risk	Low
Business Impact	This vulnerability could result in unauthorized access to critical data, leading to operational disruptions, financial losses, and reputational damage.
Mitigation	Apply the latest kernel patches and updates addressing 'Processor MMIO Stale Data' vulnerabilities. Regularly check for and apply microcode updates provided by hardware vendors.

Mitigation Strategies

This section is an overview of mitigations required to mitigate the vulnerabilities listed above.

- Strengthen passwords and disable default accounts.
- Enforce account lockout policies and monitor SSH logs.
- Apply kernel patches and hardware microcode updates.
- Disable HTTP TRACE and TRACK methods on web servers.
- Enforce SMB signing to ensure data integrity and security of SMB traffic.
- Apply kernel patches addressing 'Processor MMIO Stale Data' vulnerabilities.

Conclusion

Addressing the identified vulnerabilities is imperative for maintaining network integrity and security. The business impacts highlight the necessity for a proactive security approach and continuous adaptation to evolving threats. Implementing regular updates, monitoring, and adhering to security best practices is crucial for a robust defense mechanism. We recommend prioritizing mitigations based on the severity of business impacts and updating business continuity plans to manage these risks effectively.