Vulnerability Assessment and Penetration Testing (VAPT) Report

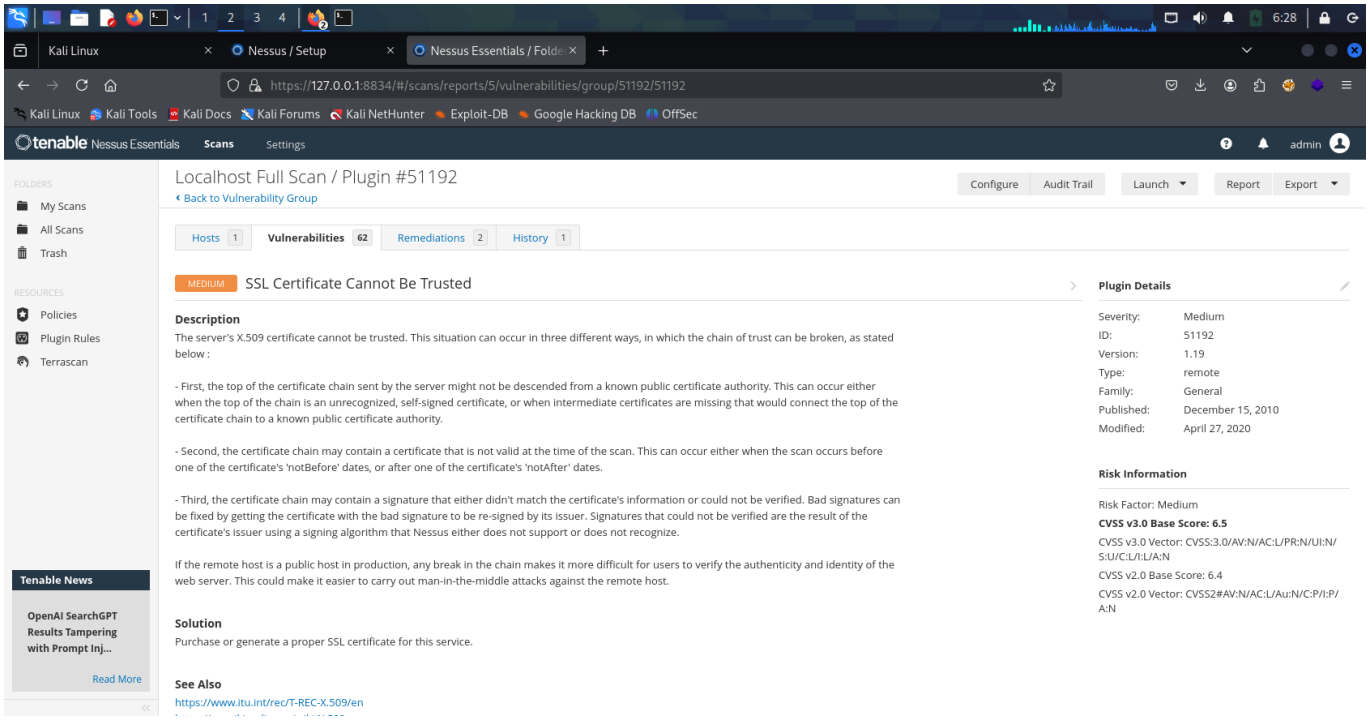
Target IP: 192.168.137.128

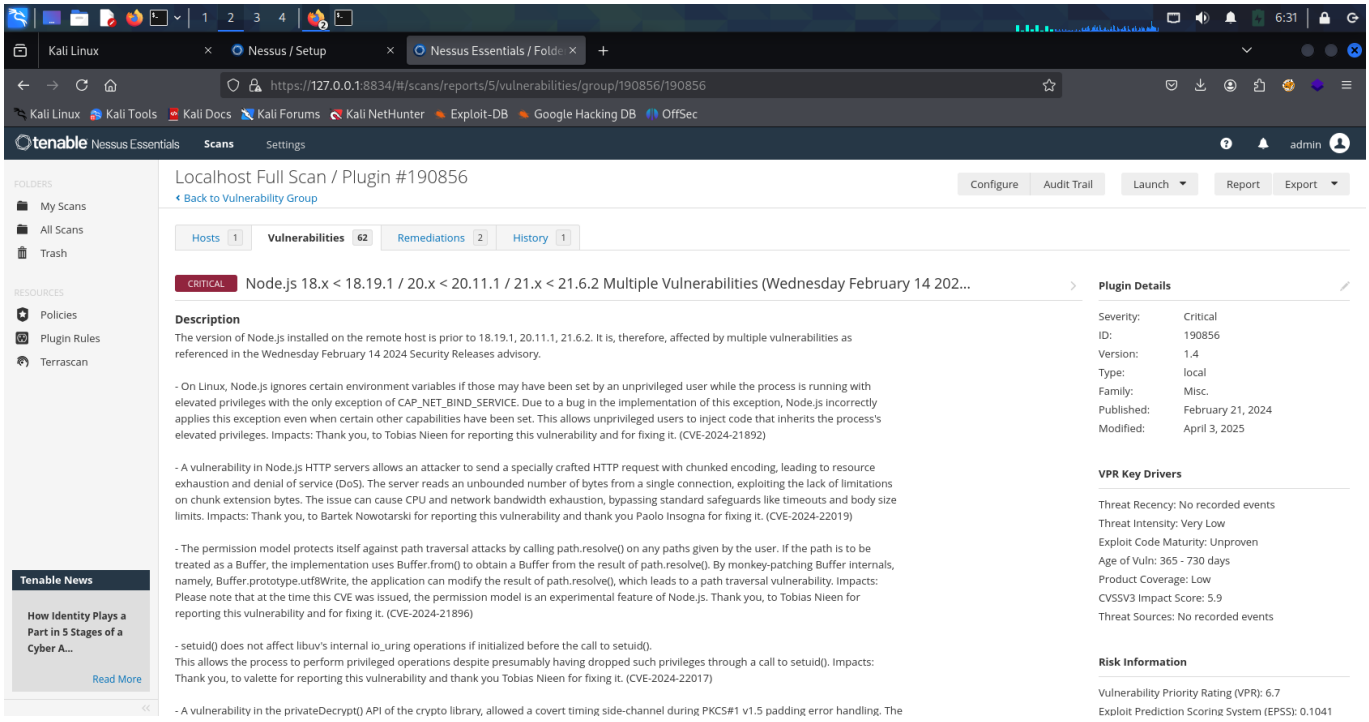
Tool Used: Nessus Essentials

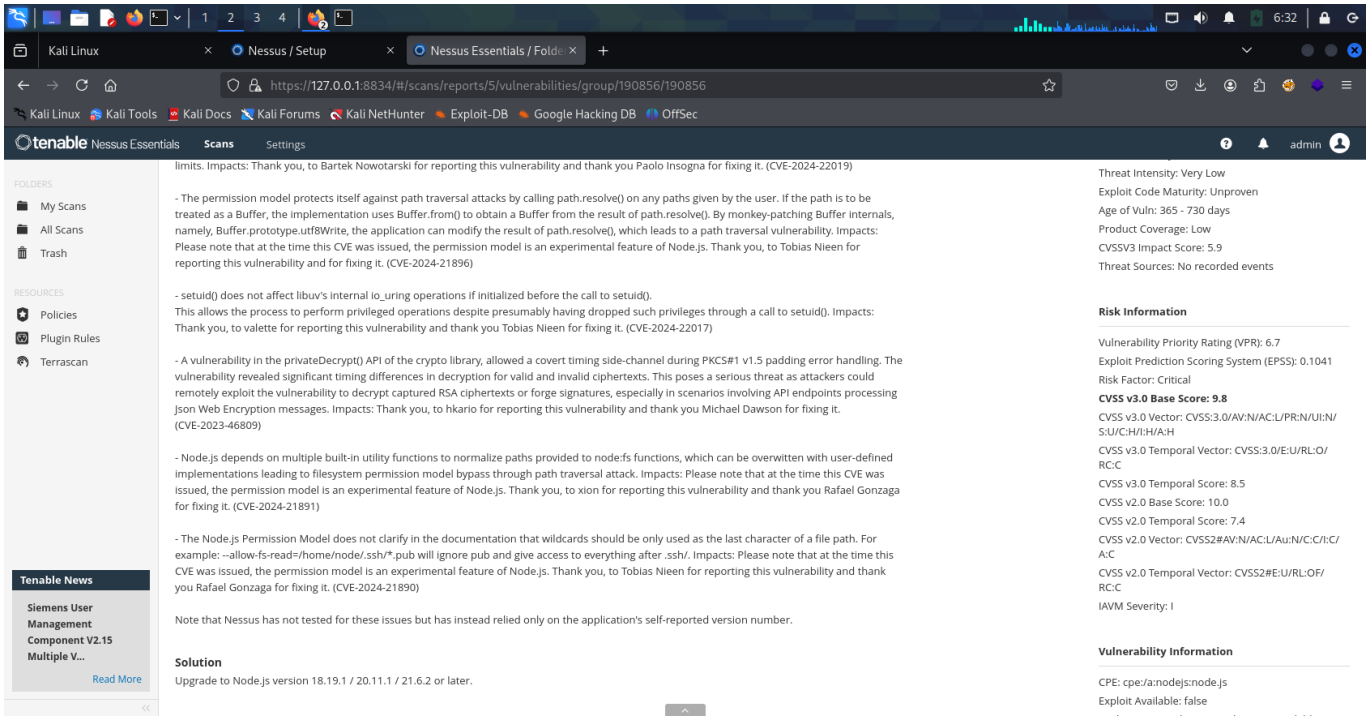
Submitted by: Sahil Rokade

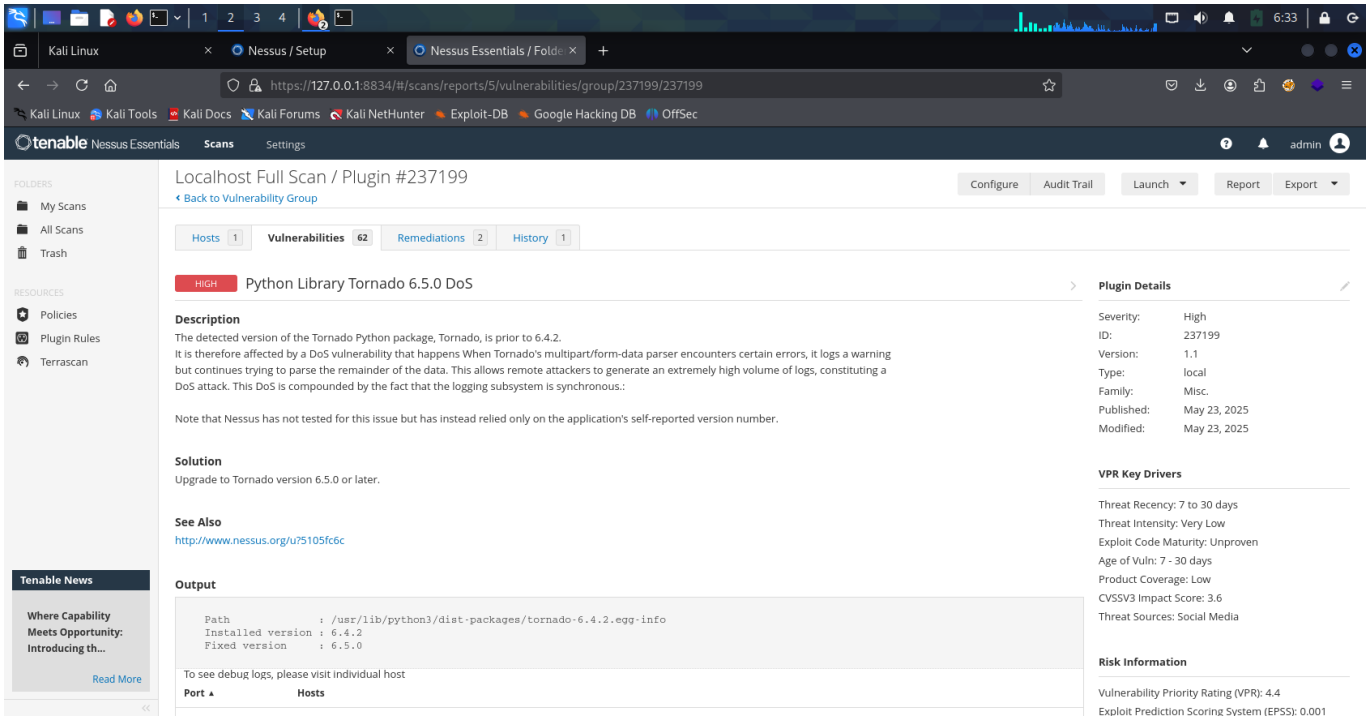
Email: sahilrokade6400@gmail.com | Phone: 9321741190

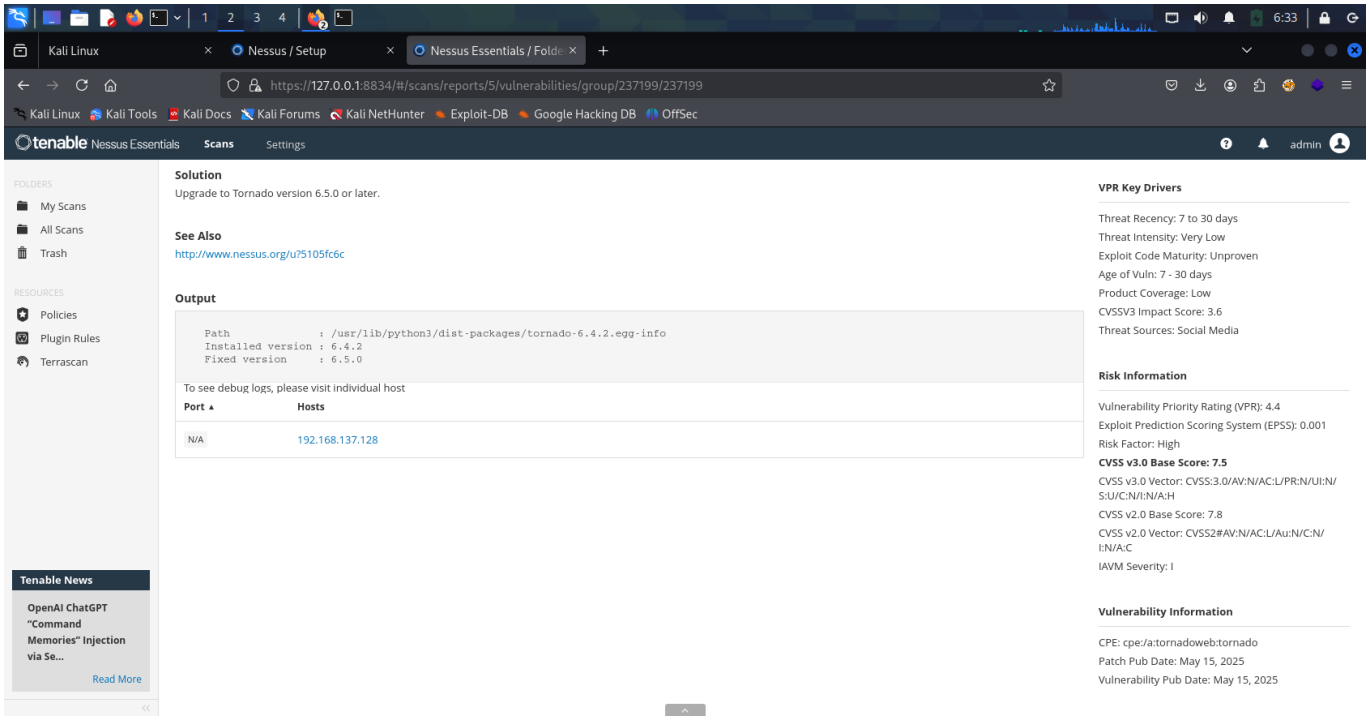
This report contains the findings of a vulnerability scan performed on a local system using Nessus Essentials. All actions were conducted in a safe, private lab environment for educational purposes.

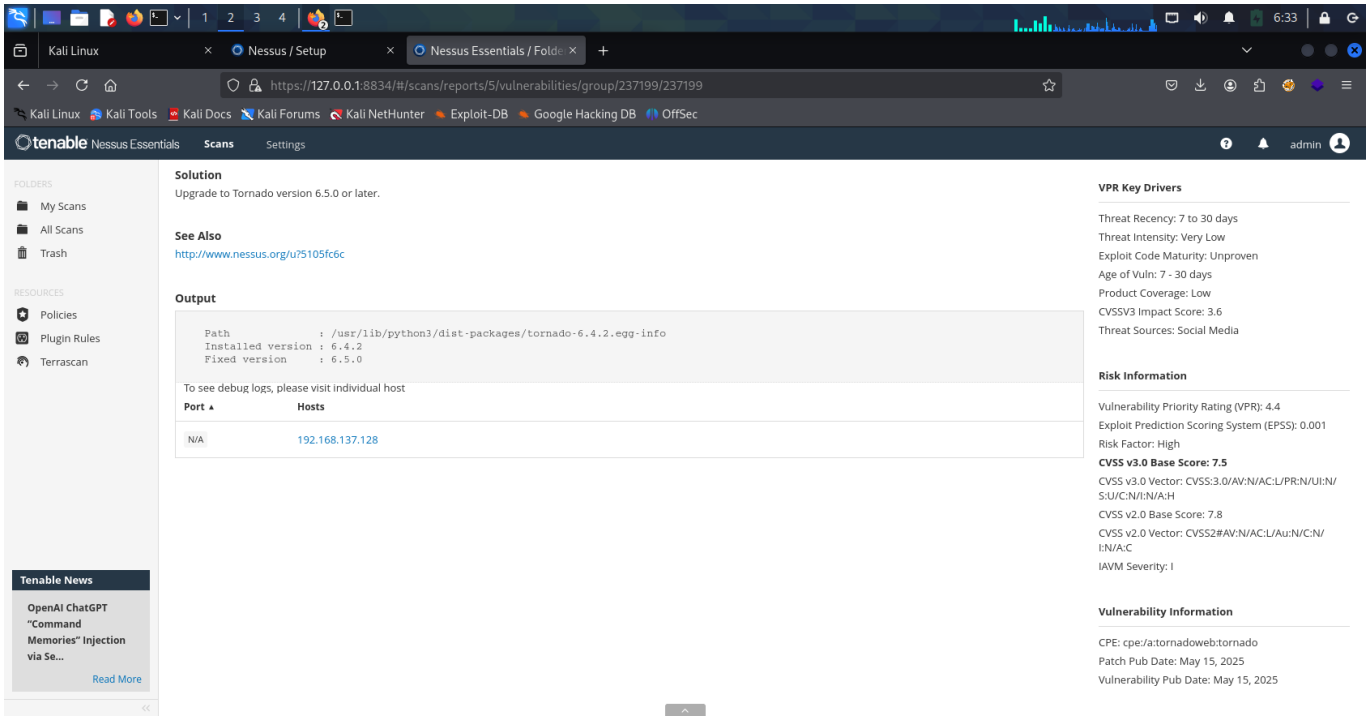

Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/51192/51192
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
OpenAI SearchGPT Results Tampering with Prompt Inj...
Read More
Localhost Full Scan / Plugin #51192
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
History 1
MEDIUM
SSL Certificate Cannot Be Trusted
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
Solution
Purchase or generate a proper SSL certificate for this service.
See Also
https://www.itu.int/rec/T-REC-X.509/en
Plugin Details
Severity: Medium
ID: 51192
Version: 1.19
Type: remote
Family: General
Published: December 15, 2010
Modified: April 27, 2020
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

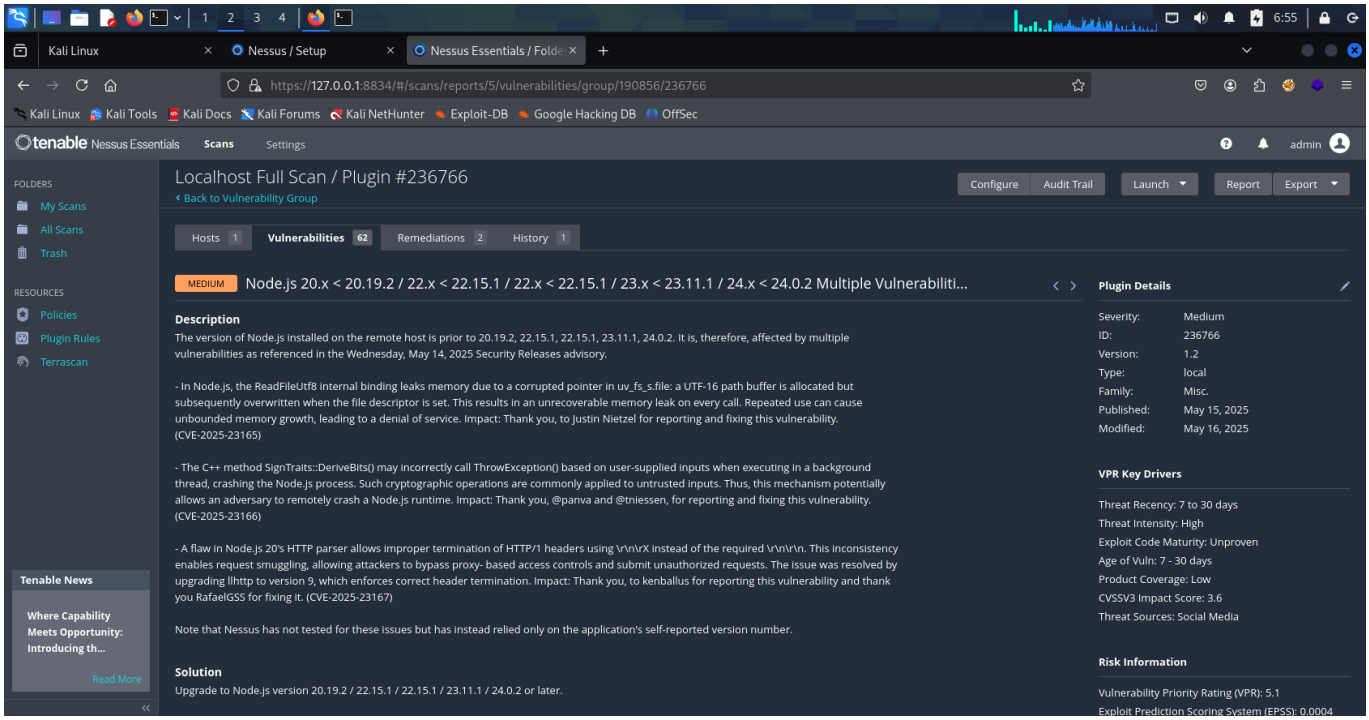

Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/190856/190856
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
How Identity Plays a Part in 5 Stages of a Cyber A...
Read More
Localhost Full Scan / Plugin #190856
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
History 1
CRITICAL
Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 202...
Description
The version of Node.js installed on the remote host is prior to 18.19.1, 20.11.1, 21.6.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday February 14 2024 Security Releases advisory.
- On Linux, Node.js ignores certain environment variables if those may have been set by an unprivileged user while the process is running with elevated privileges with the only exception of CAP_NET_BIND_SERVICE. Due to a bug in the implementation of this exception, Node.js incorrectly applies this exception even when certain other capabilities have been set. This allows unprivileged users to inject code that inherits the process's elevated privileges. Impacts: Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21892)
- A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits. Impacts: Thank you, to Bartek Nowotarski for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2024-22019)
- The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer.from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21896)
- setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid(). This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). Impacts: Thank you, to valette for reporting this vulnerability and thank you Tobias Nieen for fixing it. (CVE-2024-22017)
- A vulnerability in the privateDecrypt() API of the crypto library, allowed a covert timing side-channel during PKCS#1 v1.5 padding error handling. The
Plugin Details
Severity: Critical
ID: 190856
Version: 1.4
Type: local
Family: Misc.
Published: February 21, 2024
Modified: April 3, 2025
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 365 - 730 days
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 6.7
Exploit Prediction Scoring System (EPSS): 0.1041

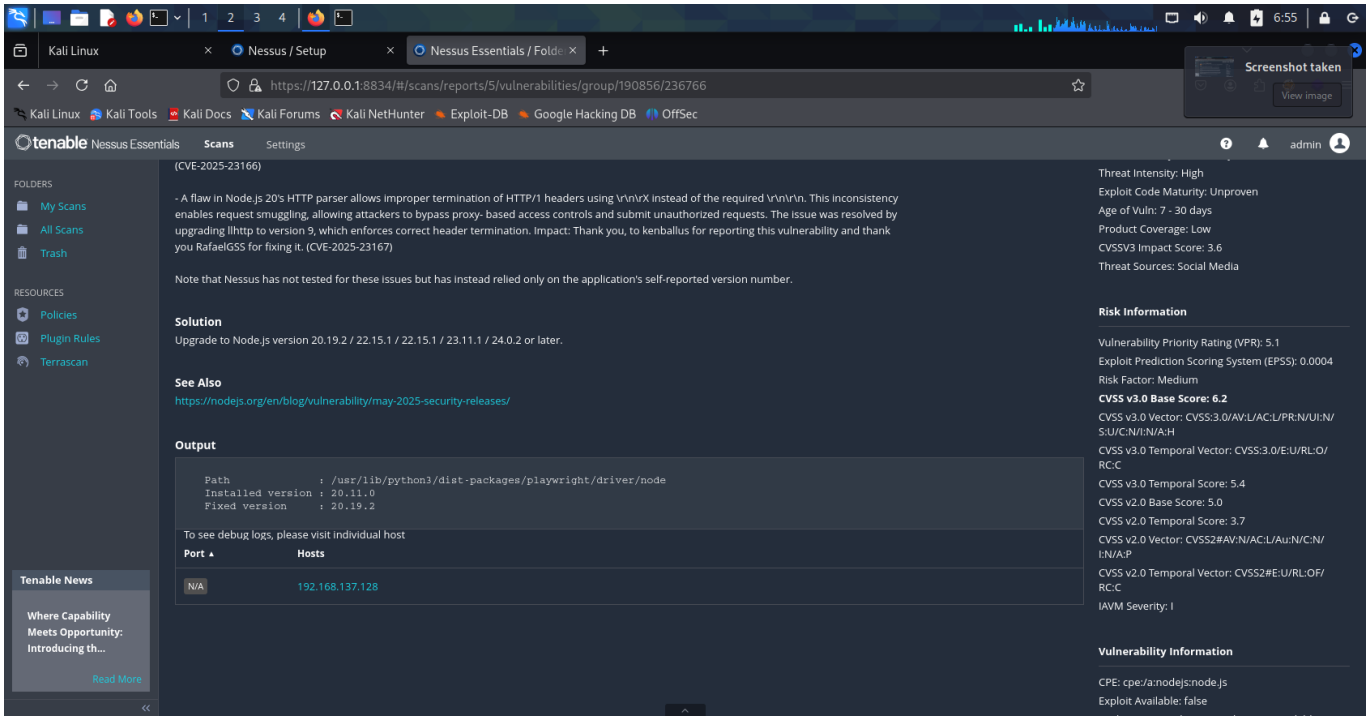

Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/190856/190856
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Siemens User Management Component V2.15 Multiple V...
Read More
limits. Impacts: Thank you, to Bartek Nowotarski for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2024-22019)
- The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer.from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21896)
- setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid(). This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). Impacts: Thank you, to valette for reporting this vulnerability and thank you Tobias Nieen for fixing it. (CVE-2024-22017)
- A vulnerability in the privateDecrypt() API of the crypto library, allowed a covert timing side-channel during PKCS#1 v1.5 padding error handling. The vulnerability revealed significant timing differences in decryption for valid and invalid ciphertexts. This poses a serious threat as attackers could remotely exploit the vulnerability to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing Json Web Encryption messages. Impacts: Thank you, to hkario for reporting this vulnerability and thank you Michael Dawson for fixing it. (CVE-2023-46809)
- Node.js depends on multiple built-in utility functions to normalize paths provided to node:fs functions, which can be overwritten with user-defined implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21891)
- The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: --allow-fs-read=/home/node/.ssh/*.pub will ignore pub and give access to everything after .ssh/. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21890)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 365 - 730 days
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 6.7
Exploit Prediction Scoring System (EPSS): 0.1041
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 7.4
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C
IAVM Severity: I
Vulnerability Information
CPE: cpe:/a:nodejs:node.js
Exploit Available: false

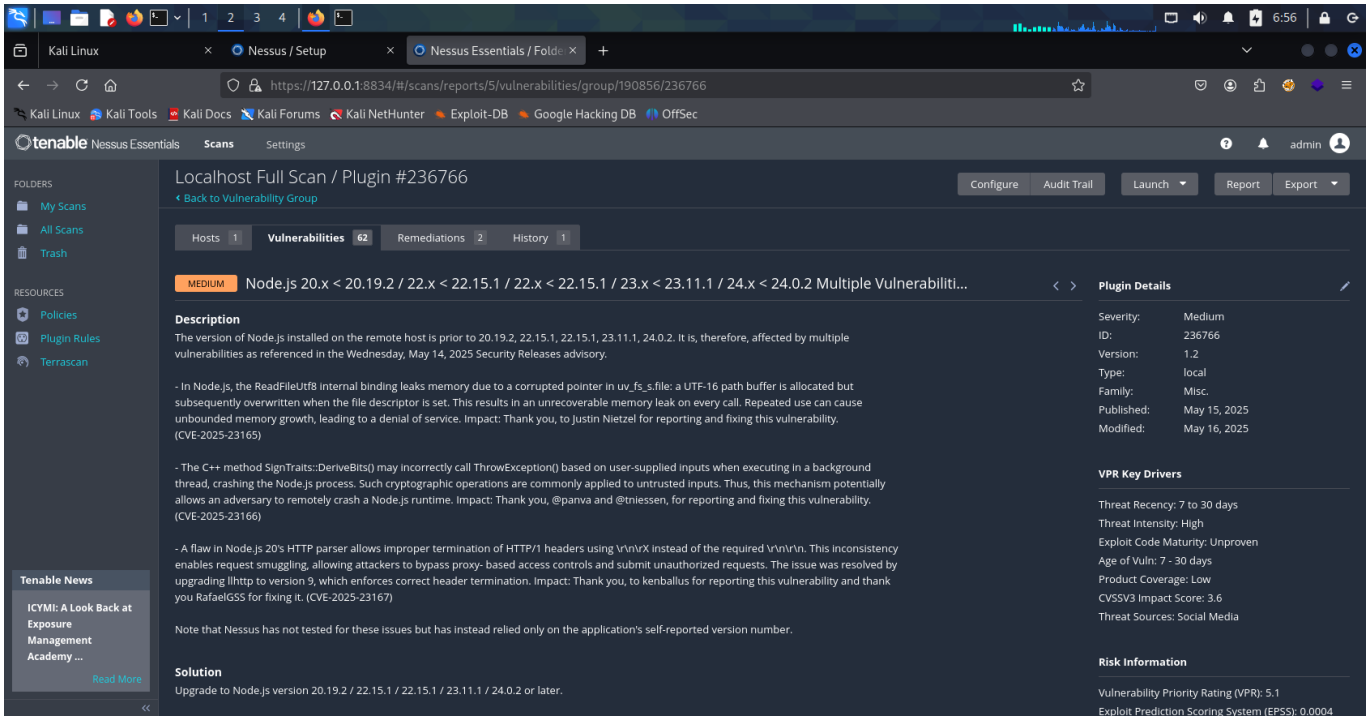

Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/237199/237199
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Where Capability Meets Opportunity: Introducing th...
Read More
Localhost Full Scan / Plugin #237199
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
History 1
HIGH
Python Library Tornado 6.5.0 DoS
Description
The detected version of the Tornado Python package, Tornado, is prior to 6.4.2.
It is therefore affected by a DoS vulnerability that happens When Tornado's multipart/form-data parser encounters certain errors, it logs a warning but continues trying to parse the remainder of the data. This allows remote attackers to generate an extremely high volume of logs, constituting a DoS attack. This DoS is compounded by the fact that the logging subsystem is synchronous.:
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Tornado version 6.5.0 or later.
See Also
http://www.nessus.org/u?5105fc6c
Output
Path : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Installed version : 6.4.2
Fixed version : 6.5.0
To see debug logs, please visit individual host
Port ▲
Hosts
Plugin Details
Severity: High
ID: 237199
Version: 1.1
Type: local
Family: Misc.
Published: May 23, 2025
Modified: May 23, 2025
VPR Key Drivers
Threat Recency: 7 to 30 days
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 4.4
Exploit Prediction Scoring System (EPSS): 0.001


Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/237199/237199
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
OpenAI ChatGPT "Command Memories" Injection via Se...
Read More
Solution
Upgrade to Tornado version 6.5.0 or later.
See Also
http://www.nessus.org/u?5105fc6c
Output
Path : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Installed version : 6.4.2
Fixed version : 6.5.0
To see debug logs, please visit individual host
Port ▲
Hosts
N/A
192.168.137.128
VPR Key Drivers
Threat Recency: 7 to 30 days
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 4.4
Exploit Prediction Scoring System (EPSS): 0.001
Risk Factor: High
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v2.0 Base Score: 7.8
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C
IAVM Severity: I
Vulnerability Information
CPE: cpe:/a:tornadoweb:tornado
Patch Pub Date: May 15, 2025
Vulnerability Pub Date: May 15, 2025


Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/237199/237199
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
OpenAI ChatGPT "Command Memories" Injection via Se...
Read More
Solution
Upgrade to Tornado version 6.5.0 or later.
See Also
http://www.nessus.org/u?5105fc6c
Output
Path : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Installed version : 6.4.2
Fixed version : 6.5.0
To see debug logs, please visit individual host
Port
Hosts
N/A
192.168.137.128
VPR Key Drivers
Threat Recency: 7 to 30 days
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 4.4
Exploit Prediction Scoring System (EPSS): 0.001
Risk Factor: High
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v2.0 Base Score: 7.8
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C
IAVM Severity: I
Vulnerability Information
CPE: cpe:/a:tornadoweb:tornado
Patch Pub Date: May 15, 2025
Vulnerability Pub Date: May 15, 2025


Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/190856/236766
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Where Capability Meets Opportunity: Introducing th...
Read More
Localhost Full Scan / Plugin #236766
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
History 1
MEDIUM
Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vulnerabiliti...
Description
The version of Node.js installed on the remote host is prior to 20.19.2, 22.15.1, 22.15.1, 23.11.1, 24.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, May 14, 2025 Security Releases advisory.
- In Node.js, the ReadFileUtf8 internal binding leaks memory due to a corrupted pointer in uv_fs_s.file: a UTF-16 path buffer is allocated but subsequently overwritten when the file descriptor is set. This results in an unrecoverable memory leak on every call. Repeated use can cause unbounded memory growth, leading to a denial of service. Impact: Thank you, to Justin Nietzel for reporting and fixing this vulnerability. (CVE-2025-23165)
- The C++ method SignTraits::DeriveBits() may incorrectly call ThrowException() based on user-supplied inputs when executing in a background thread, crashing the Node.js process. Such cryptographic operations are commonly applied to untrusted inputs. Thus, this mechanism potentially allows an adversary to remotely crash a Node.js runtime. Impact: Thank you, @panva and @tniessen, for reporting and fixing this vulnerability. (CVE-2025-23166)
- A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r\n\rX instead of the required \r\n\r\n. This inconsistency enables request smuggling, allowing attackers to bypass proxy- based access controls and submit unauthorized requests. The issue was resolved by upgrading llhttp to version 9, which enforces correct header termination. Impact: Thank you, to kenballus for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23167)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or later.
Plugin Details
Severity: Medium
ID: 236766
Version: 1.2
Type: local
Family: Misc.
Published: May 15, 2025
Modified: May 16, 2025
VPR Key Drivers
Threat Recency: 7 to 30 days
Threat Intensity: High
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 5.1
Exploit Prediction Scoring System (EPSS): 0.0004


Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/190856/236766
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Screenshot taken
View image
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Where Capability Meets Opportunity: Introducing th...
Read More
(CVE-2025-23166)
- A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r\n\rX instead of the required \r\n\r\n. This inconsistency enables request smuggling, allowing attackers to bypass proxy- based access controls and submit unauthorized requests. The issue was resolved by upgrading llhttp to version 9, which enforces correct header termination. Impact: Thank you, to kenballus for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23167)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or later.
See Also
https://nodejs.org/en/blog/vulnerability/may-2025-security-releases/
Output
Path : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version : 20.19.2
To see debug logs, please visit individual host
Port ▲
Hosts
N/A
192.168.137.128
Threat Intensity: High
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 5.1
Exploit Prediction Scoring System (EPSS): 0.0004
Risk Factor: Medium
CVSS v3.0 Base Score: 6.2
CVSS v3.0 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 5.4
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:N/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C
IAVM Severity: I
Vulnerability Information
CPE: cpe:/a:nodejs:node.js
Exploit Available: false


Kali Linux
Nessus / Setup
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/5/vulnerabilities/group/190856/236766
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
ICYMI: A Look Back at Exposure Management Academy ...
Read More
Localhost Full Scan / Plugin #236766
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 62
Remediations 2
History 1
MEDIUM
Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vulnerabiliti...
Description
The version of Node.js installed on the remote host is prior to 20.19.2, 22.15.1, 22.15.1, 23.11.1, 24.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, May 14, 2025 Security Releases advisory.
- In Node.js, the ReadFileUtf8 internal binding leaks memory due to a corrupted pointer in uv_fs_s.file: a UTF-16 path buffer is allocated but subsequently overwritten when the file descriptor is set. This results in an unrecoverable memory leak on every call. Repeated use can cause unbounded memory growth, leading to a denial of service. Impact: Thank you, to Justin Nietzel for reporting and fixing this vulnerability. (CVE-2025-23165)
- The C++ method SignTraits::DeriveBits() may incorrectly call ThrowException() based on user-supplied inputs when executing in a background thread, crashing the Node.js process. Such cryptographic operations are commonly applied to untrusted inputs. Thus, this mechanism potentially allows an adversary to remotely crash a Node.js runtime. Impact: Thank you, @panva and @tniessen, for reporting and fixing this vulnerability. (CVE-2025-23166)
- A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r\n\rX instead of the required \r\n\r\n. This inconsistency enables request smuggling, allowing attackers to bypass proxy- based access controls and submit unauthorized requests. The issue was resolved by upgrading llhttp to version 9, which enforces correct header termination. Impact: Thank you, to kenballus for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23167)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or later.
Plugin Details
Severity: Medium
ID: 236766
Version: 1.2
Type: local
Family: Misc.
Published: May 15, 2025
Modified: May 16, 2025
VPR Key Drivers
Threat Recency: 7 to 30 days
Threat Intensity: High
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: Social Media
Risk Information
Vulnerability Priority Rating (VPR): 5.1
Exploit Prediction Scoring System (EPSS): 0.0004