|  |
| --- |
| **Vulnerability Code**: **CVE-2025-23166**  **Description:**    A high-severity vulnerability (CVE-2025-23166) was discovered in Node.js affecting all active release lines (20.x, 22.x, 23.x, 24.x). The vulnerability was disclosed on May 14, 2025, and involves improper error handling in  async cryptographic operations that can lead to process crashes.  **Remediation:**  Node.js has released security updates to address this vulnerability. The fixed versions are: Node.js v20.19.2, v22.15.1, v23.11.1, and v24.0.2. Users are strongly advised to upgrade to these patched versions.  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2025-23083**  **Description:**    A high-severity vulnerability (CVE-2025-23083) was discovered in Node.js affecting versions 20, 22, and 23. The vulnerability exists in the diagnostics\_channel utility, which allows an event to be hooked into whenever a worker thread is created. This vulnerability was discovered on January 21, 2025, and affects the Permission Model users utilizing the --permission flag.  **Remediation:**  The Node.js project has released security updates to address this vulnerability. The fixed versions are: Node.js v18.20.6, v20.18.2, v22.13.1, and v23.6.1. Users are strongly advised to upgrade to these patched versions to mitigate the vulnerability  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2024-22019**  **Description:**    A vulnerability in Node.js HTTP servers (CVE-2024-22019) allows attackers to send specially crafted HTTP requests with chunked encoding, leading to resource exhaustion and denial of service (DoS). The vulnerability was discovered and disclosed in February 2024, affecting all active Node.js release lines: 18.x, 20.x, and 21.x. The issue has been assigned a CVSS v3.0 base score of 7.5 (HIGH)  **Remediation:**    The vulnerability has been patched in Node.js versions 18.19.1, 20.11.1, and 21.6.2. Users are strongly advised to upgrade to these or later versions to address the security issue  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2024-27983**  **Description:**    CVE-2024-27983 is a high-severity vulnerability affecting Node.js HTTP/2 server implementations in versions 18.x, 20.x, and 21.x. The vulnerability was discovered and disclosed in April 2024. The issue allows an attacker to make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with HTTP/2 CONTINUATION frames  **Remediation:**    The vulnerability has been patched in Node.js versions 20.12.1 and later. The fix ensures to close the stream when destroying the session. Organizations using affected versions should upgrade to the patched versions immediately. The fix was contributed by Anna Henningsen  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2024-21891**  **Description:**    Node.js versions prior to 20.11.1 and 21.6.2 contain a vulnerability in the experimental permission model where built-in utility functions used to normalize paths provided to node:fs functions can be overwritten with user-defined implementations. This vulnerability was discovered in early 2024 and affects all users using the experimental permission model in Node.js 20 and Node.js 21 release lines  **Remediation:**    The vulnerability has been patched in Node.js versions 20.11.1 and 21.6.2. Users running affected versions should upgrade to these patched versions or later. Since this vulnerability specifically affects the experimental permission model, users who are not using this feature are not impacted  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2024-22017**  **Description:**    A high-severity vulnerability (CVE-2024-22017) was discovered in Node.js affecting versions 18.18.0 and later, 20.4.0 and later, and version 21. The vulnerability relates to the setuid() function not properly affecting libuv's internal io\_uring operations when initialized before the setuid() call  **Remediation:**  The vulnerability has been addressed in the February 2024 security releases of Node.js. Users are advised to upgrade to the patched versions: Node.js 20.11.1 for the v20.x series and appropriate security updates for other affected versions  **Steps:**   1. Check the node version by running node -v powershell   If output shows a **20.x ≤ 20.19.1**, **22.x ≤ 22.15.0**, **23.x ≤ 23.11.0**, or **24.x ≤ 24.0.1**, Node.js is vulnerable.   1. Download and install a patched Node.js version via:    1. Official installer (.msi)    2. Package managers like **nvm-windows** or **Chocolatey** 2. Confirm post-update: run node -v in powershell |
| **Vulnerability Code**:**CVE-2024-21896**  **Description:**    The vulnerability (CVE-2024-21896) affects Node.js versions 20.x and 21.x, specifically targeting the experimental permission model. Discovered and disclosed in February 2024, this high-severity vulnerability allows path traversal attacks through manipulation of Buffer internals  **Remediation:**  The vulnerability has been patched in Node.js version 20.11.1 and subsequent releases. Users are strongly recommended to upgrade to these patched versions. Red Hat has also released security updates to address this vulnerability in their Enterprise Linux distributions  **Steps:**   1. Check the node version by running node -v shell  If the version is below:  * **v20.11.1** for Node.js 20 * **v21.6.2** for Node.js 21  1. Download and install a patched Node.js version:  * **v20.11.1 or later** * **v21.6.2 or later**  1. Confirm post-update: run node -v in shell |
| **Vulnerability Code**:**CVE-2016-10540**  **Description:**    **CVE-2016-10540** is a **Regular Expression Denial of Service (ReDoS)** vulnerability in the minimatch Node.js library (version ≤ 3.0.1). It occurs when complex glob patterns are translated into inefficient regular expressions that cause **excessive backtracking,** which can freeze or slow down the application.  **Remediation:**  Mitigation of CVE-2016-10540 involves applying foundational **security principles** to prevent or reduce the impact of **ReDoS (Regular Expression Denial of Service)** attacks.  **steps:** run the following command **npm update minimatch** |
| **Vulnerability Code**:**CVE-2024-45296**  **Description:**  path-to-regexp is a package that turns path strings into regular expressions. A vulnerability was discovered where in certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. The vulnerability affects versions prior to 0.1.10, 0.2.0 prior to 1.9.0, 2.0.0 prior to 3.3.0, 4.0.0 prior to 6.3.0, and 7.0.0 prior to 8.0.0.  .  **Remediation:**  For users of 0.1, upgrade to 0.1.10. All other users should upgrade to 8.0.0. These versions add backtrack protection when a custom regex pattern is not provided. For versions that cannot be upgraded, a workaround is to provide a custom regular expression for parameters after the first in a single segment. For example, change /:a-:b to /:a-:b([**-/**](https://www.wiz.io/vulnerability-database/cve/cve-2024-45296#-)+).  **steps:**  Upgrade path-to-regexp to:   * ≥ 0.1.10, or * ≥ 1.9.0, or * ≥ 3.3.0, or * ≥ 6.3.0, or * ≥ 8.0.0 depending on the current major version |
| **Vulnerability Code**:**CVE-2024-4068**  **Description:**  The NPM package braces, versions prior to 3.0.3, contains a vulnerability that fails to limit the number of characters it can handle, potentially leading to Memory Exhaustion. This vulnerability is tracked as CVE-2024-4068 and was discovered in early 2024  **Remediation:**  The vulnerability has been fixed in version 3.0.3 of the braces package. The fix includes reducing the default maxLength to 10,000 characters, which provides adequate protection against memory exhaustion attacks while maintaining functionality for legitimate use cases  **Steps:**  Upgrade to fixed version:  **npm install braces@3.0.3 --save** |
| **Vulnerability Code**:**CVE-2025-4918**  **Description:**  CVE-2025-4918 is a critical security vulnerability discovered in Mozilla Firefox that allows attackers to perform an out-of-bounds read or write operation on a JavaScript Promise object. The vulnerability was identified on May 17, 2025, and affects Firefox versions < 138.0.4, Firefox ESR < 128.10.1, Firefox ESR < 115.23.1, Thunderbird < 128.10.2, and Thunderbird < 138.0.2. The flaw was discovered by Edouard Bochin and Tao Yan from Palo Alto Networks working with Trend Micro's Zero Day Initiative  .  **Remediation:**    Mozilla has released security updates to address this vulnerability. Users and administrators are advised to update their Firefox installations to version 138.0.4, Firefox ESR to version 128.10.1 or 115.23.1, and Thunderbird to version 128.10.2 or 138.0.2 as soon as possible  **Steps:**   * Upgrade to Firefox 138.0.4 or later * Upgrade to Firefox ESR 128.10.1 or 115.23.1 or later * Update Thunderbird to 128.10.2 or later, or non‑ESR to 138.0.2 or later |
| **Vulnerability Code**:**CVE-2025-4919**  **Description:**  CVE-2025-4919 is a critical security vulnerability discovered in Mozilla Firefox that was disclosed on May 17, 2025. The vulnerability affects Firefox versions before 138.0.4, Firefox ESR versions before 128.10.1 and 115.23.1, Thunderbird versions before 128.10.2 and 138.0.2. The flaw allows an attacker to perform an out-of-bounds read or write on a JavaScript object by confusing array index sizes  **Remediation:**  Mozilla has released patches for all affected versions. Users are advised to update to Firefox 138.0.4, Firefox ESR 128.10.1, Firefox ESR 115.23.1, Thunderbird 128.10.2, or Thunderbird 138.0.2 as appropriate. Mozilla emphasizes that all users and administrators should update Firefox as soon as possible to mitigate the risk  **Steps:**   * Upgrade to Firefox 138.0.4 or later * Upgrade to Firefox ESR 128.10.1 or 115.23.1 or later * Update Thunderbird to 128.10.2 or later, or non‑ESR to 138.0.2 or later |
| **Vulnerability Code**:**CVE-2024-9394**  **Description:**  CVE-2024-9394 is a high-severity security vulnerability discovered in Mozilla products that affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. The vulnerability was disclosed on October 1, 2024, and was reported by security researcher Masato Kinugawa  **Remediation:**  Mozilla has addressed this vulnerability in Firefox 131, Firefox ESR 128.3, Firefox ESR 115.16, Thunderbird 128.3, and Thunderbird 131. Users are advised to update their software to these or later versions to mitigate the risk  **Steps:**   * Upgrade to Firefox 138.0.4 or later * Upgrade to Firefox ESR 128.10.1 or 115.23.1 or later * Update Thunderbird to 128.10.2 or later, or non‑ESR to 138.0.2 or later |
| **Vulnerability Code**:**CVE-2024-9393**  **Description:**    CVE-2024-9393 is a high-severity vulnerability discovered in Mozilla products that was disclosed on October 1, 2024. The vulnerability affects multiple versions of Mozilla products including Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131. The issue was discovered by security researcher Masato Kinugawa  **Remediation:**  Mozilla has addressed this vulnerability in Firefox 131, Firefox ESR 128.3, Firefox ESR 115.16, Thunderbird 128.3, and Thunderbird 131. Users are advised to update their software to these or later versions to mitigate the risk  **Steps:**   * Upgrade to Firefox 138.0.4 or later * Upgrade to Firefox ESR 128.10.1 or 115.23.1 or later * Update Thunderbird to 128.10.2 or later, or non‑ESR to 138.0.2 or later |
| **Vulnerability Code:CVE-2024-4367**  **Description:**    A type check vulnerability (CVE-2024-4367) was discovered in PDF.js that allows arbitrary JavaScript execution in the PDF.js context. The vulnerability affects Firefox versions before 126, Firefox ESR versions before 115.11, and Thunderbird versions before 115.11. The issue was discovered by Thomas Rinsma of Codean Labs and was publicly disclosed on May 14, 2024    **Remediation:**  The vulnerability has been fixed in Firefox 126, Firefox ESR 115.11, and Thunderbird 115.11. For PDF.js library users, the fix is available in version 4.2.67. The fix involves implementing proper type validation for font matrix values before they are used in JavaScript code generation  **Steps:**   * **For Browsers:**   + Update Firefox to version 126 or later.   + Update Firefox ESR to 115.11 or later.   + Update Thunderbird to 115.11 or later.[support.mozilla.org+10mozilla.org+10sploitus.com+10](https://www.mozilla.org/en-US/security/advisories/mfsa2024-21/?utm_source=chatgpt.com) * **For Applications Using PDF.js:**   + Upgrade to pdfjs-dist v4.2.67 or newer.   + Alternatively, disable JavaScript evaluation within PDF.js by configuring:   pdfjsLib.GlobalWorkerOptions.isEvalSupported = false; |
| **Vulnerability Code:CVE-2024-3853**  **Description:**  CVE-2024-3853 is a high-severity use-after-free vulnerability discovered in Mozilla Firefox. The vulnerability was identified by Gary Kwong and affects Firefox versions prior to 125. The issue occurs when a JavaScript realm is in the process of being initialized during garbage collection operations  **Remediation:**    The vulnerability has been fixed in Firefox version 125. Users are advised to update their Firefox installations to version 125 or later to mitigate this security risk. The fix involves keeping realms alive if they are in the process of being initialized at the start of garbage collection  **Steps:**   * Upgrade to Firefox 125.0.4 or later |
| **Vulnerability Code:CVE-2024-5694**  **Description:**  CVE-2024-5694 is a security vulnerability affecting Mozilla Firefox versions prior to 127. The vulnerability was discovered by Lukas Bernhard and disclosed on June 11, 2024. It affects the JavaScript engine in Firefox, specifically involving a use-after-free condition in the JavaScript string section of the heap  **Remediation:**  The vulnerability has been fixed in Firefox version 127. Users are advised to update to this version or later to mitigate the risk. The fix was released as part of Mozilla's regular security update cycle  **Steps:**   * Upgrade to Firefox 127.0.0 or later |
| **Vulnerability Code:CVE-2024-29944**  **Description:**  CVE-2024-29944 is a critical vulnerability in Mozilla Firefox discovered and reported by Manfred Paul via Trend Micro's Zero Day Initiative. The vulnerability was disclosed on March 22, 2024, affecting Desktop Firefox versions prior to 124.0.1 and Firefox ESR versions prior to 115.9.1. This security flaw does not affect mobile versions of Firefox  **Remediation:**    Mozilla has released patches in Firefox 124.0.1 and Firefox ESR 115.9.1 to address this vulnerability. Users are strongly advised to update their Desktop Firefox installations to these versions or later. The fix involves avoiding the registration of unnecessary MessageManager listeners when SHIP is enabled  **Steps:**   * Upgrade to Firefox 124.0.0 or later * Upgrade to Firefox ESR 128.10.1 or 115.9.1 or later |
| **Vulnerability Code:CVE-2024-3858**  **Description:**  CVE-2024-3858 is a security vulnerability discovered in Firefox versions prior to 125 that involves a JavaScript object mutation issue. The vulnerability was disclosed on April 16, 2024, affecting the Firefox browser's JavaScript engine, specifically its Just-In-Time (JIT) compiler component  **Remediation:**    The vulnerability has been fixed in Firefox version 125. Users are advised to update to Firefox 125 or later to receive the security fix. The fix involves modifying the TraceWeakCacheIRStub function to ensure all fields are properly traced  **Steps:**   * Upgrade to Firefox 125.0.0 or later |
| **Vulnerability Code:CVE-2025-4083**  **Description:**  CVE-2025-4083 is a process isolation vulnerability discovered in Mozilla Firefox and Thunderbird that was disclosed on April 29, 2025. The vulnerability affects Firefox < 138, Firefox ESR < 128.10, Firefox ESR < 115.23, Thunderbird < 138, and Thunderbird ESR < 128.10. The vulnerability was discovered by security researcher Nika Layzell  **Remediation:**  Mozilla has addressed this vulnerability in Firefox 138, Firefox ESR 128.10, Firefox ESR 115.23, Thunderbird 138, and Thunderbird ESR 128.10. Users are advised to update their installations to these versions or newer to mitigate the risk  **Steps:**   * Upgrade to Firefox 138.0.4 or later * Upgrade to Firefox ESR 128.10.1 or 115.23.1 or later * Update Thunderbird to 128.10.2 or later, or non‑ESR to 138.0.2 or later |
| **Vulnerability Code:CVE-2024-29943**  **Description:**  CVE-2024-29943 is a critical vulnerability discovered in Firefox versions prior to 124.0.1, disclosed on March 22, 2024. The vulnerability allows an attacker to perform an out-of-bounds read or write on a JavaScript object by fooling range-based bounds check elimination  **Remediation:**    Mozilla has addressed this vulnerability in Firefox version 124.0.1. Users are strongly advised to update to this version or later. The fix involved removing the problematic MObjectKeysLength::computeRange optimization code, which has been verified to not significantly impact performance  **Steps:**   * Upgrade to Firefox 124.0.1 or later |
| **Vulnerability Code:CVE-2024-8384**  **Description:**  CVE-2024-8384 is a vulnerability in the JavaScript garbage collector affecting multiple Mozilla products including Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15. The vulnerability was discovered by the Mozilla Fuzzing Team and publicly disclosed on September 3, 2024  **Remediation:**    The vulnerability has been fixed in Firefox 130, Firefox ESR 128.2, Firefox ESR 115.15, Thunderbird 128.2, and Thunderbird 115.15. Users are advised to update to these versions or later to mitigate the vulnerability  **Steps:**   * Upgrade to Firefox 130.0.1 or later * Upgrade to Firefox ESR 128.2.0 or 115.23.1 or later * Update Thunderbird to 128.2.0 or later, or non‑ESR to 138.0.2 or later |