Vulnerabilities found:

- CVE ID: NVD

  Description: Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability

  CVSS Score: 4.0

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 5.1

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

No vulnerabilities found.----------Vulnerabilities found:

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description: [jQuery](https://jquery.com/) ? New Wave JavaScript

==========...

  CVSS Score: 4.3

- CVE ID: exploit

  Description: [jQuery](http://jquery.com/) - New Wave JavaScript

==========...

  CVSS Score: 4.3

- CVE ID: exploit

Description: # CVE-2020-11022 CVE-2020-11023

> In jQuery versions greater th...

CVSS Score: 4.3

- CVE ID: exploit

Description: This repository contains the patches for [CVE-2020-11022](https:...

CVSS Score: 6.5

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: NVD

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: NVD

Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

CVSS Score: 4.3

- CVE ID: NVD

Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e.

.html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS Score: 4.3

- CVE ID: NVD

Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS Score: 4.3

- CVE ID: NVD

Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

CVSS Score: 4.3

- CVE ID: NVD

Description: The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.

CVSS Score: 5.0

- CVE ID: NVD

Description: The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service

(ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.

CVSS Score: 5.0

- CVE ID: NVD

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: NVD

Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

CVSS Score: 4.3

- CVE ID: NVD

Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` are vulnerable to cross-site scripting. This occurs because the main `jquery` function uses a regular expression to differentiate between HTML and selectors, but does not properly anchor the regular expression. The result is that `jquery` may interpret HTML as selectors when given certain inputs, allowing for client side code execution.

Proof of Concept

```
$("#log").html(
  $("element[attribute='<img src=\"x\" onerror=\"alert(1)\" />']").html()
);
```

Recommendation

Update to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: software

Description: Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove `<script>` HTML tags that contain a whitespace character, i.e: `</script >`, which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Recommendation

Upgrade to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` interpret `text/javascript` responses from cross-origin ajax requests, and automatically execute the contents in `jQuery.globalEval`, even when the ajax request doesn't contain the `dataType` option.

Recommendation

Update to version 3.0.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: ## Overview

Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Recommendation

Upgrade to version 1.9.0 or later.

References

- [GitHub Advisory](https://github.com/advisories/GHSA-q4m3-2j7h-f7xw)
  CVSS Score: 4.3

- CVE ID: software
  Description: Affected versions of `jquery` are vulnerable to cross-site scripting. This occurs because the main `jquery` function uses a regular expression to differentiate between HTML and selectors, but does not properly anchor the regular expression. The result is that `jquery` may interpret HTML as selectors when given certain inputs, allowing for client side code execution.

Proof of Concept

```
$("#log").html(
  $("element[attribute='<img src=\"x\" onerror=\"alert(1)\" />']").html()
);
```

```

## Recommendation

Update to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: software

Description: Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove `&lt;script&gt;` HTML tags that contain a whitespace character, i.e: `&lt;/script &gt;`, which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

## Recommendation

Upgrade to version 1.9.0 or later.
```

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` interpret `text/javascript` responses from cross-origin ajax requests, and automatically execute the contents in `jQuery.globalEval`, even when the ajax request doesn't contain the `dataType` option.

Recommendation

Update to version 3.0.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: jquery is vulnerable to cross-site scripting (XSS). The regular expression in `load()` method does not properly remove HTML tags containing a whitespace character in the closing script tag (e.g `

CVSS Score: 4.3

No vulnerabilities found.

----------Vulnerabilities found:

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description:

CVSS Score: 4.3

- CVE ID: exploit

Description: [jQuery](https://jquery.com/) ? New Wave JavaScript

==========...

CVSS Score: 4.3

- CVE ID: exploit

Description: [jQuery](http://jquery.com/) - New Wave JavaScript

==========...

CVSS Score: 4.3

- CVE ID: exploit

Description: # CVE-2020-11022 CVE-2020-11023

> In jQuery versions greater th...

CVSS Score: 4.3

- CVE ID: exploit

Description: This repository contains the patches for [CVE-2020-11022](https:...

CVSS Score: 6.5

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: exploit

  Description:

  CVSS Score: 4.3

- CVE ID: NVD

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: NVD

Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

CVSS Score: 4.3

- CVE ID: NVD

Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS Score: 4.3

- CVE ID: NVD

Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS Score: 4.3

- CVE ID: NVD

Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

CVSS Score: 4.3

- CVE ID: NVD

Description: The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.

CVSS Score: 5.0

- CVE ID: NVD

Description: The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.

CVSS Score: 5.0

- CVE ID: NVD

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: NVD

Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

CVSS Score: 4.3

- CVE ID: NVD

Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` are vulnerable to cross-site scripting. This occurs because the main `jquery` function uses a regular expression to differentiate between HTML and selectors, but does not properly anchor the regular expression. The result is that `jquery` may interpret HTML as selectors when given certain inputs, allowing for client side code execution.

Proof of Concept

```
```

```
$("#log").html(
    $("element[attribute='<img src=\"x\" onerror=\"alert(1)\" />']").html()
);
```

Recommendation

Update to version 1.9.0 or later.
  CVSS Score: 4.3

- CVE ID: software
    Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.
  CVSS Score: 4.3

- CVE ID: software
   Description: Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove `<script>` HTML tags that contain a whitespace character, i.e: `</script >`, which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Recommendation

Upgrade to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` interpret `text/javascript` responses from cross-origin ajax requests, and automatically execute the contents in `jQuery.globalEval`, even when the ajax request doesn't contain the `dataType` option.

Recommendation

Update to version 3.0.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: ## Overview

Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Recommendation

Upgrade to version 1.9.0 or later.

References

- [GitHub Advisory](https://github.com/advisories/GHSA-q4m3-2j7h-f7xw)
  CVSS Score: 4.3

- CVE ID: software
  Description: Affected versions of `jquery` are vulnerable to cross-site scripting. This occurs because the main `jquery` function uses a regular expression to differentiate between HTML and selectors, but does not properly anchor the regular expression. The result is that `jquery` may interpret HTML as selectors when given certain inputs, allowing for client side code execution.

Proof of Concept

```
$("#log").html(
  $("element[attribute='<img src=\"x\" onerror=\"alert(1)\" />']").html()
);
```

Recommendation

Update to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

CVSS Score: 4.3

- CVE ID: software

Description: Versions of `jquery` prior to 1.9.0 are vulnerable to Cross-Site Scripting. The load method fails to recognize and remove `<script>` HTML tags that contain a whitespace character, i.e: `</script >`, which results in the enclosed script logic to be executed. This allows attackers to execute arbitrary JavaScript in a victim's browser.

Recommendation

Upgrade to version 1.9.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: Affected versions of `jquery` interpret `text/javascript` responses from cross-origin ajax requests, and automatically execute the contents in `jQuery.globalEval`, even when the ajax request doesn't contain the `dataType` option.

Recommendation

Update to version 3.0.0 or later.

CVSS Score: 4.3

- CVE ID: software

Description: jquery is vulnerable to cross-site scripting (XSS). The regular expression in `load()` method does not properly remove HTML tags containing a whitespace character in the closing script tag (e.g `

CVSS Score: 4.3

No vulnerabilities found.----------Vulnerabilities found:

- CVE ID: exploit

Description:

CVSS Score: 5.5

- CVE ID: exploit

Description: File disclosure vulnerability in WordPress Slider Revolution Responsive plugin

Vulnerability Type: File Disclosure

CVSS Score: 5.0

- CVE ID: exploit

Description:

CVSS Score: 5.5

- CVE ID: exploit

  Description:

  CVSS Score: 10.0

- CVE ID: exploit

  Description:

  CVSS Score: 7.5

- CVE ID: exploit

  Description:

  CVSS Score: 5.0

- CVE ID: exploit

  Description:

  CVSS Score: 5.5

- CVE ID: exploit

  Description:

  CVSS Score: 7.5

- CVE ID: NVD

  Description: Multiple cross-site scripting (XSS) vulnerabilities in template-functions-post.php in WordPress 1.5 and earlier allow remote attackers to execute arbitrary commands via the (1) content or (2) title of the post.

  CVSS Score: 6.8

- CVE ID: NVD

Description: Wordpress 1.5 and earlier allows remote attackers to obtain sensitive information via a direct request to files in (1) wp-content/themes/, (2) wp-includes/, or (3) wp-admin/, which reveal the path in an error message.

CVSS Score: 5.0

- CVE ID: NVD

Description: A flaw exists in Wordpress related to the 'wp-admin/press-this.php 'script improperly checking user permissions when publishing posts. This may allow a user with 'Contributor-level' privileges to post as if they had 'publish_posts' permission.

CVSS Score: 4.0

- CVE ID: NVD

Description: In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 3.5

- CVE ID: NVD

Description: In affected versions of WordPress, files with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 3.5

- CVE ID: NVD

Description: In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 5.5

- CVE ID: NVD

Description: In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 4.3

- CVE ID: NVD

Description: In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 4.3

- CVE ID: NVD

Description: In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVSS Score: 3.5

- CVE ID: software

Description: HackApp vulnerability scanner discovered that application WordPress published at the 'play' market has multiple vulnerabilities.

CVSS Score: 0.0

- CVE ID: software

Description: WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions the widgets editor introduced in WordPress 5.8 beta 1 has improper handling of HTML input in the Custom HTML feature. This leads to stored XSS in the custom HTML widget. This has been patched in WordPress 5.8. It was only present during the testing/beta phase of WordPress 5.8.

CVSS Score: 3.5

- CVE ID: software

Description: WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. In affected versions authenticated users who don't have permission to view private post types/data can bypass restrictions in the block editor under certain conditions. This affected WordPress 5.8 beta during the testing period. It's fixed in the final 5.8

release.

CVSS Score: 6.0

- CVE ID: software

Description: Because of these vulnerabilities in wp-login.php, the attackers can change the content of the forgotten password e-mail message via the message variable, that is not initialized before use.

Solution

Update the WordPress to the latest available version (at least 1.5.1.3).

CVSS Score: 5.0

- CVE ID: software

Description: Because of this vulnerability, attackers can obtain sensitive information.

Solution

Update WordPress to the latest possible version.

CVSS Score: 5.0

- CVE ID: software

Description: Becase of these vulnerabilities, the attackers can determine the existence of arbitrary files and possibly read portions of certain files.

Solution

Update the WordPress to the latest available version (at least 1.4.6).

CVSS Score: 5.0

- CVE ID: software

Description: Because of this vulnerability in wp-login.php, attackers can perform HTTP Response Splitting attacks to modify expected HTML content from the server via the "text" parameter.

Solution

Update the WordPress to the latest available version (at least 1.2.1).

CVSS Score: 5.0

- CVE ID: software

Description: Because of this vulnerability, attackers can execute arbitrary SQL commands via the $cat_ID variable.

Solution

Update the WordPress to the latest available version (at least 1.5.2).

CVSS Score: 7.5

- CVE ID: software

Description: WordPress version prior to 1.5.1.3 is remotely exploitable if the web server on which it runs has register_globals enabled in the PHP configuration. Perl code exists to automatically exploit vulnerable WP 1.5.1.3 sites, allowing the attacker to try to execute code.

Solution

Update WordPress.

CVSS Score: 7.5

- CVE ID: software

Description: Because of these vulnerabilities, attackers can inject arbitrary web script or HTML.

Solution

Update WordPress to the latest possible version.

CVSS Score: 4.3

- CVE ID: software

Description: Because of this vulnerability, the authenticated users with manage_options and upload_files capabilities can execute arbitrary code by uploading a PHP script.

Solution

Update WordPress.

CVSS Score: 8.5

- CVE ID: software

Description: Because of these vulnerabilities, the attackers can obtain sensitive information via a direct request to wp-admin/upgrade-functions.php, wp-includes/vars.php, wp-admin/edit-form.php, wp-content/plugins/hello.php, wp-settings.php or wp-admin/edit-form-comment.php.

Solution

Update the WordPress to the latest available version (at least 1.5.2).

CVSS Score: 5.0

- CVE ID: software

Description: This vulnerability is in sidebar.php. It allows the attackers to inject arbitrary web script or HTML via the query string.

Solution

Update WordPress.

CVSS Score: 6.8

- CVE ID: software

Description: Because of this vulnerability in wp-admin/vars.php, the authenticated users with theme privileges can inject arbitrary web script or HTML via the PATH_INFO.

Solution

Update the WordPress to the latest available version (at least 2.1.3).

CVSS Score: 4.3

- CVE ID: software

Description: Because of this vulnerability, the attackers can inject arbitrary web script or HTML via the "id" parameter.

Solution

Update the plugin.

CVSS Score: 4.3

- CVE ID: software

Description: Because of these vulnerabilities, the attackers can obtain sensitive information via a direct request to menu-header.php or a value in the "feed" parameter to wp-atom.php.

Solution

Update the Wordpress to the latest available version (at least 1.5.1.3).

CVSS Score: 5.0

- CVE ID: software

Description: Because of this vulnerability, the attackers can redirect authenticated users to other websites and potentially obtain sensitive information.

Solution

Update the WordPress to the latest available version (at least 1.1).

CVSS Score: 6.5

- CVE ID: software

Description: Because of this vulnerability in The _httpsrequest function in Snoopy, the attackers can execute arbitrary commands via shell metacharacters in an HTTPS URL to an SSL protected web page, that is not properly handled by the fetch function.

Solution

Update the WordPress to the latest available version (at least 1.3).

CVSS Score: 7.5

- CVE ID: software

Description: Because of this vulnerability, attackers can execute arbitrary SQL commands via the User-Agent field in an HTTP header for a comment.

Solution

Update the WordPress to the latest available version (at least 1.5.3).

CVSS Score: 7.5

- CVE ID: software

Description: Because of this vulnerability, attackers can inject arbitrary web script or HTML.

Solution

Update the WordPress to the latest available version (at least 1.5.3).

CVSS Score: 6.8

- CVE ID: software

Description: Because of this vulnerability in wp-trackback.php, attackers can execute arbitrary SQL commands via the "tb_id" parameter.

Solution

Update this plugin.

CVSS Score: 7.5

- CVE ID: software

Description: Because of these vulnerabilities in template-functions-post.php, attackers can execute arbitrary commands via the title of the post or content.

Solution

Update WordPress to the latest possible version.

CVSS Score: 6.8

- CVE ID: software

Description: Because of these vulnerabilities in post.php, attackers can inject arbitrary web script or HTML via the "p" or "comment" parameter.

Solution

Update the WordPress to the latest available version (at least 1.5.1.3).

CVSS Score: 4.3

- CVE ID: software

Description: Multiple WordPress themes are prone to an arbitrary file download vulnerability. It allows an attacker to download arbitrary files from the web server and get potentially sensitive information.

Solution

Upgrade themes.

CVSS Score: 5.0

- CVE ID: software

Description: Because of this vulnerability in XMLRPC server, attackers can execute arbitrary SQL commands via input that is not filtered in the HTTP_RAW_POST_DATA variable, which stores the data in an XML file.

Solution

Update the WordPress to the latest available version (at least 1.5.1.3).

CVSS Score: 7.5

- CVE ID: software

Description:

CVSS Score: 7.5

- CVE ID: software

Description:

CVSS Score: 5.0

- CVE ID: software

Description:

CVSS Score: 7.5

- CVE ID: software

Description:

CVSS Score: 4.3

- CVE ID: software

Description:

CVSS Score: 7.5

- CVE ID: software

Description:

CVSS Score: 7.5

No vulnerabilities found.----------Vulnerabilities found:

- CVE ID: NVD

Description: Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability

CVSS Score: 4.0

- CVE ID: NVD

Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 5.1

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

- CVE ID: NVD

  Description: Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability

  CVSS Score: 6.8

No vulnerabilities found.--Vulnerabilities found:

- CVE ID: NVD

  Description: PHP5 before 5.4.4 allows passing invalid utf-8 strings via the xmlTextWriterWriteAttribute, which are then misparsed by libxml2. This results in memory leak into the resulting output.

  CVSS Score: 5.0

- CVE ID: NVD

Description: SQL injection vulnerability in Zend Framework 1.10.x before 1.10.9 and 1.11.x before 1.11.6 when using non-ASCII-compatible encodings in conjunction PDO_MySql in PHP before 5.3.6.

CVSS Score: 7.5

- CVE ID: NVD

Description: Use-after-free vulnerability in the add_post_var function in the Posthandler component in PHP 5.6.x before 5.6.1 might allow remote attackers to execute arbitrary code by leveraging a third-party filter extension that accesses a certain ksep value.

CVSS Score: 6.8

No vulnerabilities found.----------Vulnerabilities found:

- CVE ID: exploit

Description: # CVE-2024-27316 (HTTP/2 CONTINUATION flood) PoC

Target serv...

CVSS Score: 0.0

- CVE ID: exploit

Description: # CVE-2023-44487-

----------...

CVSS Score: 5.0

- CVE ID: exploit

Description: # HTTP/2 Rapid Reset: CVE-2023-44487

Description

This repos...

CVSS Score: 5.0

- CVE ID: exploit

Description: # Golang CVE-2023-44487 testing

This repository contains testin...

CVSS Score: 5.0

- CVE ID: exploit

Description: # CVE-2023-44487

Basic vulnerability scanning to see if web serv...

CVSS Score: 5.0

- CVE ID: exploit

Description: # CVE-2024-27316

I decided to call this vulnerability specifica...

CVSS Score: 0.0

- CVE ID: exploit

Description: # CVE-2023-44487 (HTTP/2 Rapid Reset)

There are some examples i...

CVSS Score: 5.0

- CVE ID: exploit

Description: # HTTP2 Rapid Reset Attack: CVE-2023-44487

Quick exploit to test...

CVSS Score: 5.0

- CVE ID: exploit

Description: # HTTP/2 Rapid Reset Client (C#)

The HTTP/2 Rapid Reset Client,...

CVSS Score: 5.0

- CVE ID: software

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS Score: 6.4

- CVE ID: software

Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS Score: 5.0

- CVE ID: software

Description: Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.This issue affects Apache HTTP Server: through 2.4.58.

CVSS Score: 0.0

- CVE ID: software

Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.Users are recommended to upgrade to version 2.4.59, which fixes this issue.

CVSS Score: 0.0

- CVE ID: software

Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

CVSS Score: 0.0

No vulnerabilities found.

----------Vulnerabilities found:

- CVE ID: NVD

Description: PHP5 before 5.4.4 allows passing invalid utf-8 strings via the xmlTextWriterWriteAttribute, which are then misparsed by libxml2. This results in memory leak into the resulting output.

CVSS Score: 5.0

- CVE ID: NVD

Description: SQL injection vulnerability in Zend Framework 1.10.x before 1.10.9 and 1.11.x before 1.11.6 when using non-ASCII-compatible encodings in conjunction PDO_MySql in PHP before 5.3.6.

CVSS Score: 7.5

- CVE ID: NVD

Description: Use-after-free vulnerability in the add_post_var function in the Posthandler component in PHP 5.6.x before 5.6.1 might allow remote attackers to execute arbitrary code by leveraging a third-party filter extension that accesses a certain ksep value.

CVSS Score: 6.8

No vulnerabilities found.----------Vulnerabilities found:

- CVE ID: exploit

  Description: # CVE-2024-27316 (HTTP/2 CONTINUATION flood) PoC

Target serv...

  CVSS Score: 0.0

- CVE ID: exploit

  Description: # CVE-2023-44487-

----------...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # HTTP/2 Rapid Reset: CVE-2023-44487

Description

This repos...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # Golang CVE-2023-44487 testing

This repository contains testin...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # CVE-2023-44487

Basic vulnerability scanning to see if web serv...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # CVE-2024-27316

I decided to call this vulnerability specifica...

  CVSS Score: 0.0

- CVE ID: exploit

  Description: # CVE-2023-44487 (HTTP/2 Rapid Reset)

There are some examples i...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # HTTP2 Rapid Reset Attack: CVE-2023-44487

Quick exploit to test...

  CVSS Score: 5.0

- CVE ID: exploit

  Description: # HTTP/2 Rapid Reset Client (C#)

The HTTP/2 Rapid Reset Client,...

CVSS Score: 5.0

- CVE ID: software

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS Score: 6.4

- CVE ID: software

Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS Score: 5.0

- CVE ID: software

Description: Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.This issue affects Apache HTTP Server: through 2.4.58.

CVSS Score: 0.0

- CVE ID: software

Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection

busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS Score: 5.0

- CVE ID: software

Description: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.Users are recommended to upgrade to version 2.4.59, which fixes this issue.

CVSS Score: 0.0

- CVE ID: software

Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

CVSS Score: 0.0

No vulnerabilities found.----------