Critical Threats in Modern Systems
Step 1 - Preliminary Data Model

Jair Ramirez

CS 4332 Introduction to Database Systems

Texas State University

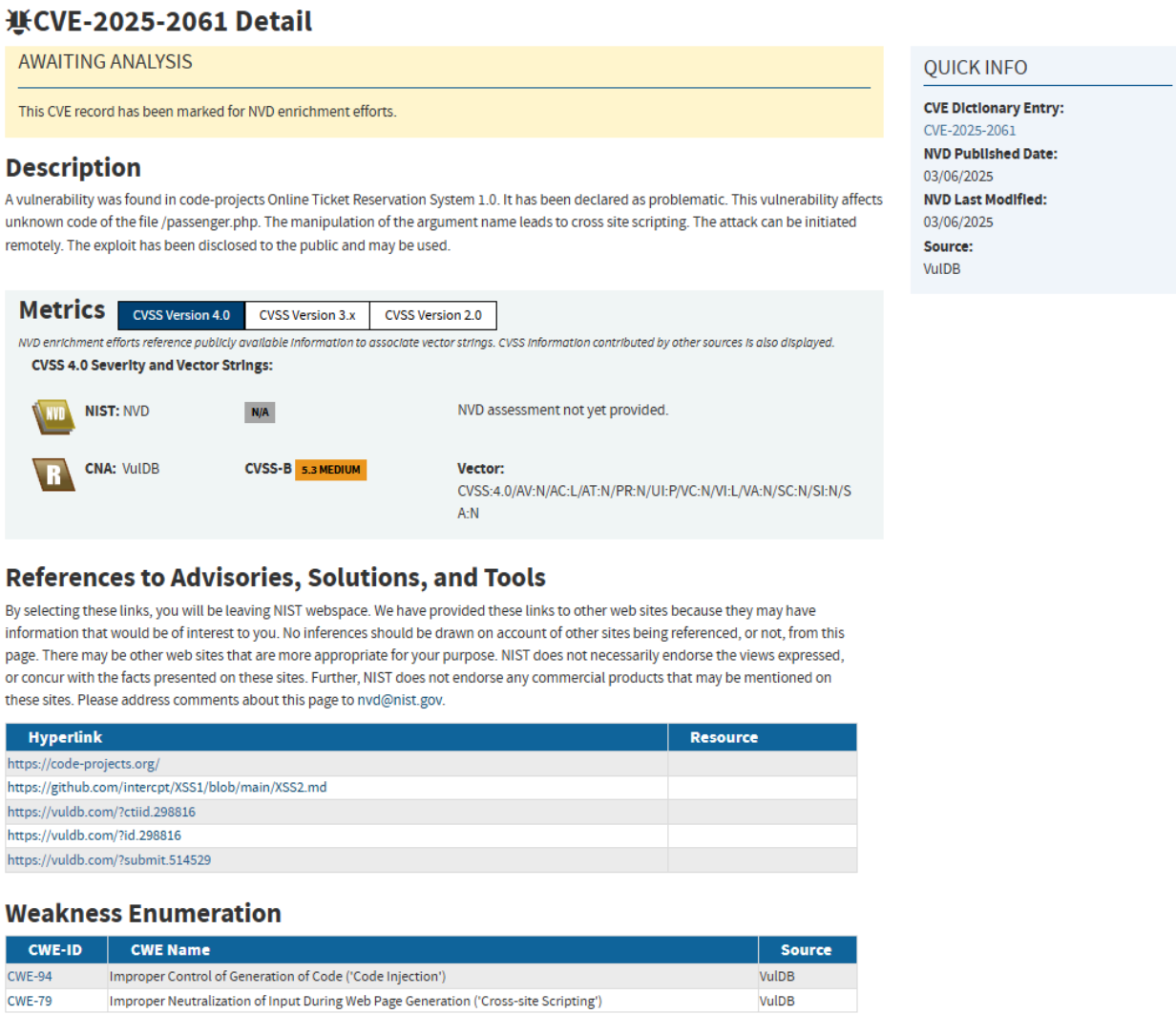
March 31st, 2025

Abstract

This step develops the logical data model for our Critical Threats in Modern Systems vulnerability database. We first review the business reports and source documents to identify core entities (e.g., Vulnerability, Product, Advisory) and their attributes. Next, we construct an Entity-Relationship diagram and translate it into a normalized relational schema in the third normal form. The resulting model ensures data integrity, supports efficient querying of CVE details and related mitigation strategies, and lays the groundwork for implementation for the next step.

Section A - Reports & Data

In this section, we gather raw input materials—business forms, vulnerability advisories, and sample reports—from authoritative sources (e.g., NVD's CVE listings and vendor security bulletins). These documents define the entities and attributes we'll model in our database schema.



CVE-2025-2061 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

QUICK INFO

CVE Dictionary Entry: CVE-2025-2061
NVD Published Date: 03/06/2025
NVD Last Modified: 03/06/2025
Source: VulDB

Description

A vulnerability was found in code-projects Online Ticket Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD — N/A — NVD assessment not yet provided.

CNA: VulDB — **CVSS-B** 5.3 MEDIUM — **Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://code-projects.org/	
https://github.com/intercpt/XSS1/blob/main/XSS2.md	
https://vuldb.com/?ctiid.298816	
https://vuldb.com/?id.298816	
https://vuldb.com/?submit.514529	

Weakness Enumeration

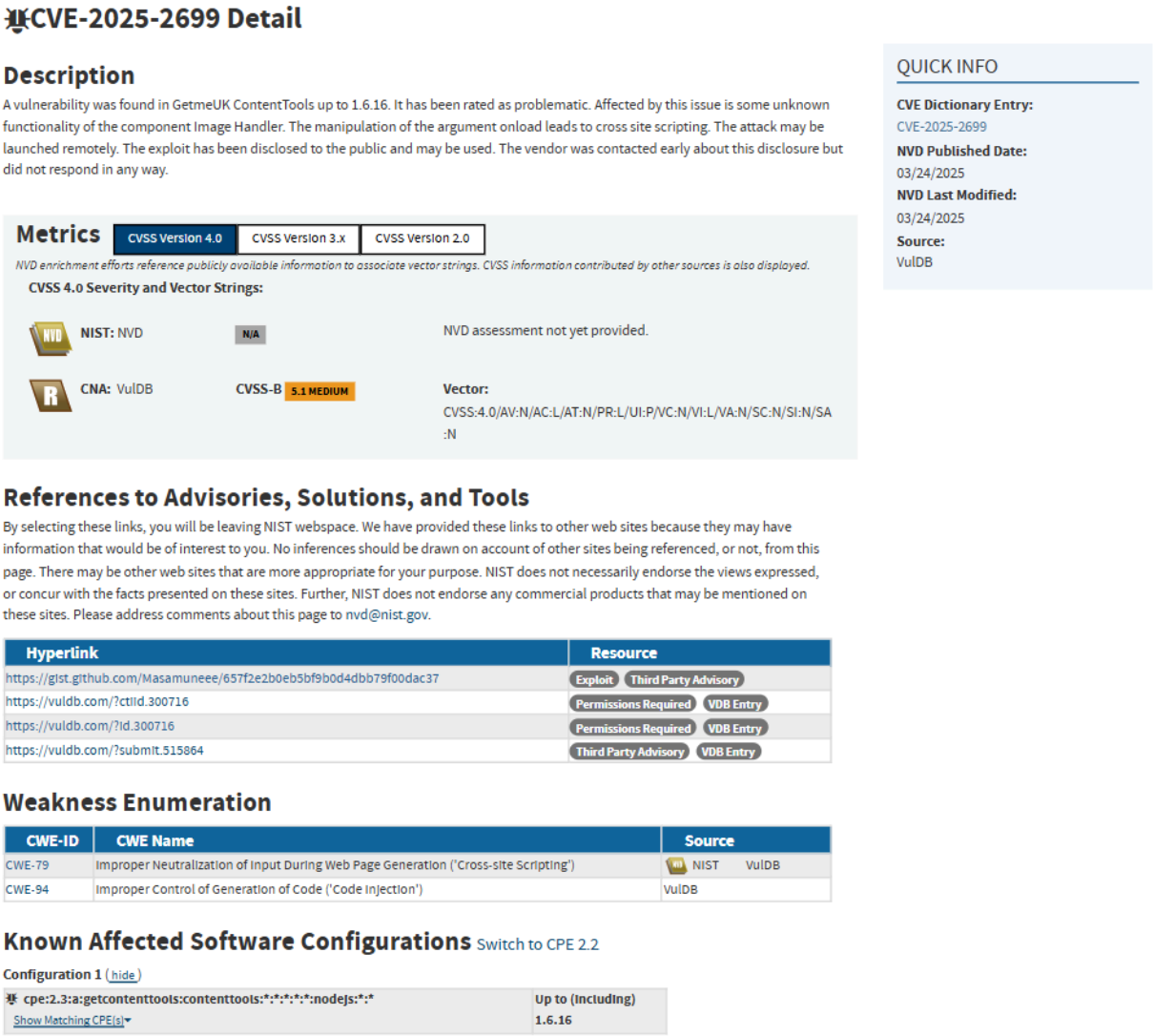
CWE-ID	CWE Name	Source
CWE-94	Improper Control of Generation of Code ('Code Injection')	VulDB
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	VulDB

Figure 1: NIST Advisory for CVE-2025-2061 (Cross-Site Scripting Vulnerability)

Figure 1 presents a snapshot from the NIST Vulnerability Database detailing **CVE-2025-2061**. It highlights a Cross-Site Scripting (XSS) flaw in the **Online Ticket Reservation System 1.0**, along with its CVSS severity score, relevant references, and the potential consequences of the vulnerability.

- **CVE ID**: *CVE-2025-2061*

- **Vulnerability Type**: *Cross-Site Scripting*
- **CVSS Score / Severity**: *CVSS 5.3 Medium* (as shown in the figure)
- **ProductName**: *Online Ticket Reservation System*
- **Version**: *1.0*
- **Vendor**: Code-projects
- **Description**: This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name leads to cross site scripting.
- **Impact**: Exploitation of this vulnerability allows remote attackers to inject and execute malicious scripts in the context of a user's browser. This can lead to session hijacking, unauthorized actions, or theft of sensitive information.
- **Mitigation**: Implement proper input validation and output encoding on the affected file (/passenger.php). Sanitize all user-supplied data to ensure special characters are handled safely, and apply secure coding practices to prevent script injection.
- **DiscoveryDate**:2025-03-06



CVE-2025-2699 Detail

Description

A vulnerability was found in GetmeUK ContentTools up to 1.6.16. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Image Handler. The manipulation of the argument onload leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

QUICK INFO

CVE Dictionary Entry: CVE-2025-2699
NVD Published Date: 03/24/2025
NVD Last Modified: 03/24/2025
Source: VulDB

Metrics: CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD — N/A — NVD assessment not yet provided.

CNA: VulDB — CVSS-B 5.1 MEDIUM — Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://gist.github.com/Masamuneee/657f2e2b0eb5bf9b0d4dbb79f00dac37	Exploit, Third Party Advisory
https://vuldb.com/?ctiId.300716	Permissions Required, VDB Entry
https://vuldb.com/?id.300716	Permissions Required, VDB Entry
https://vuldb.com/?submit.515864	Third Party Advisory, VDB Entry

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	NIST, VulDB
CWE-94	Improper Control of Generation of Code ('Code Injection')	VulDB

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

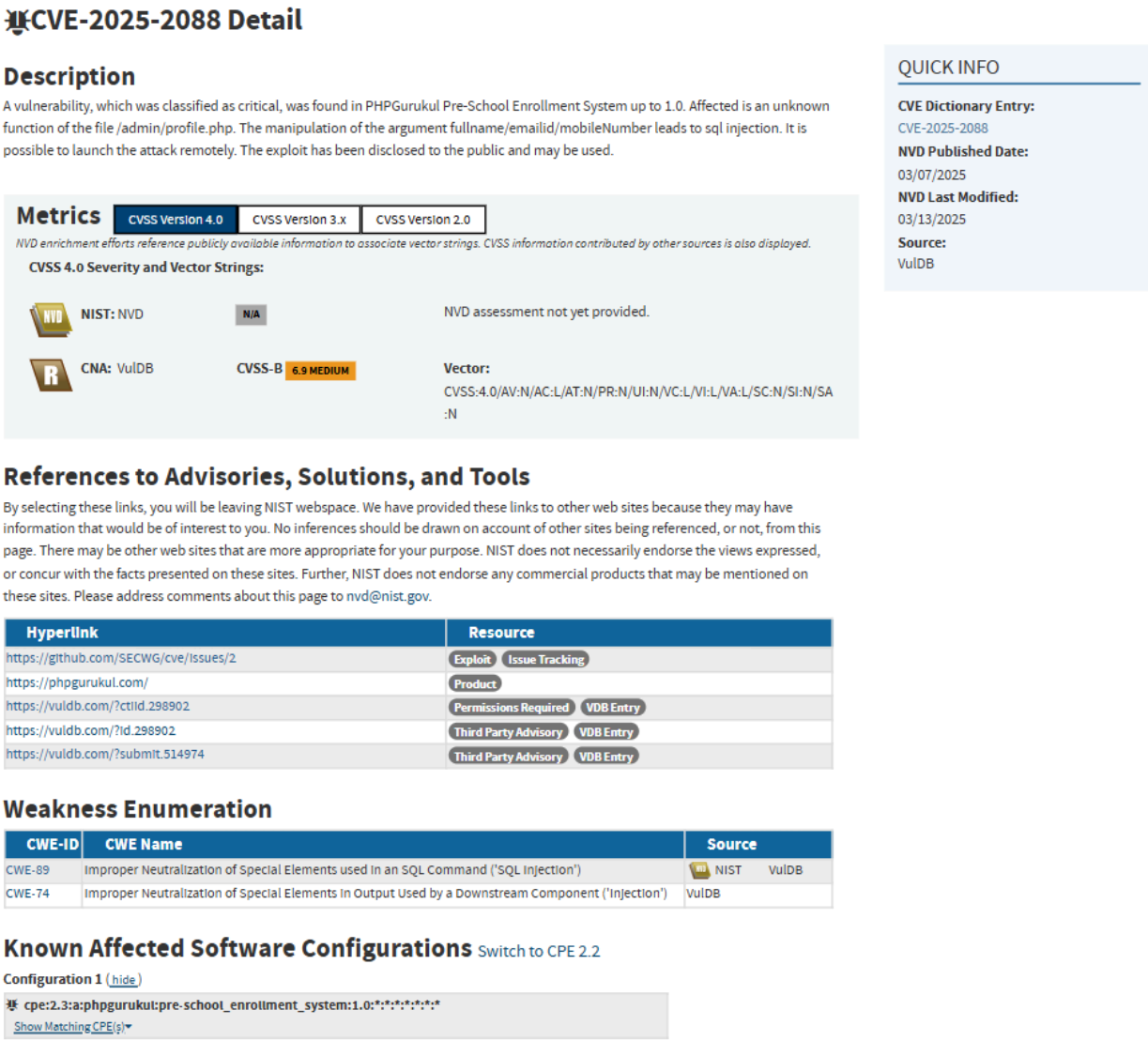
cpe:2.3:a:getcontenttools:contenttools:*:*:*:*:*:nodejs:*:*	Up to (including) 1.6.16
Show Matching CPE(s)	

Figure 2: NIST Advisory for CVE-2025-2699 (Cross-Site Scripting Vulnerability)

Figure 2 displays a NIST Vulnerability Database entry for **CVE-2025-2699**, describing a Cross-Site Scripting (XSS) vulnerability discovered in **GetmeUK Content Tools (<= v1.6.16)**. The entry provides critical information including:

- **CVE Identifier:** *CVE-2025-2699*
- **Vulnerability Type:** *Cross-Site Scripting (XSS)*
- **CVSS Score / Severity:** *CVSS 5.1 Medium (as shown in the figure)*

- **ProductName**: *ContentTools*
- **Version**: *<= 1.6.16*
- **Vendor**: *GetmeUK*
- **Description**: Affected by this issue is some unknown functionality of the component Image Handler. The manipulation of the argument onload leads to cross site scripting.
- **Impact**: Exploitation of this vulnerability can allow remote attackers to inject and execute malicious scripts via the onload parameter, potentially leading to session hijacking, unauthorized data access, or client-side attacks such as phishing.
- **Mitigation**: Apply strict input validation and output encoding for the onload attribute in the Image Handler component. Additionally, review and patch the affected component in GetmeUK ContentTools.
- **DiscoveryDate**: 2025-03-24



CVE-2025-2088 Detail

Description

A vulnerability, which was classified as critical, was found in PHPGurukul Pre-School Enrollment System up to 1.0. Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

QUICK INFO

CVE Dictionary Entry: CVE-2025-2088
NVD Published Date: 03/07/2025
NVD Last Modified: 03/13/2025
Source: VulDB

Metrics — CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD — N/A — NVD assessment not yet provided.

CNA: VulDB — CVSS-B 6.9 MEDIUM — Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/SECWG/cve/issues/2	Exploit, Issue Tracking
https://phpgurukul.com/	Product
https://vuldb.com/?ctiid.298902	Permissions Required, VDB Entry
https://vuldb.com/?id.298902	Third Party Advisory, VDB Entry
https://vuldb.com/?submit.514974	Third Party Advisory, VDB Entry

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	NIST, VulDB
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	VulDB

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:phpgurukul:pre-school_enrollment_system:1.0:*:*:*:*:*:*:*

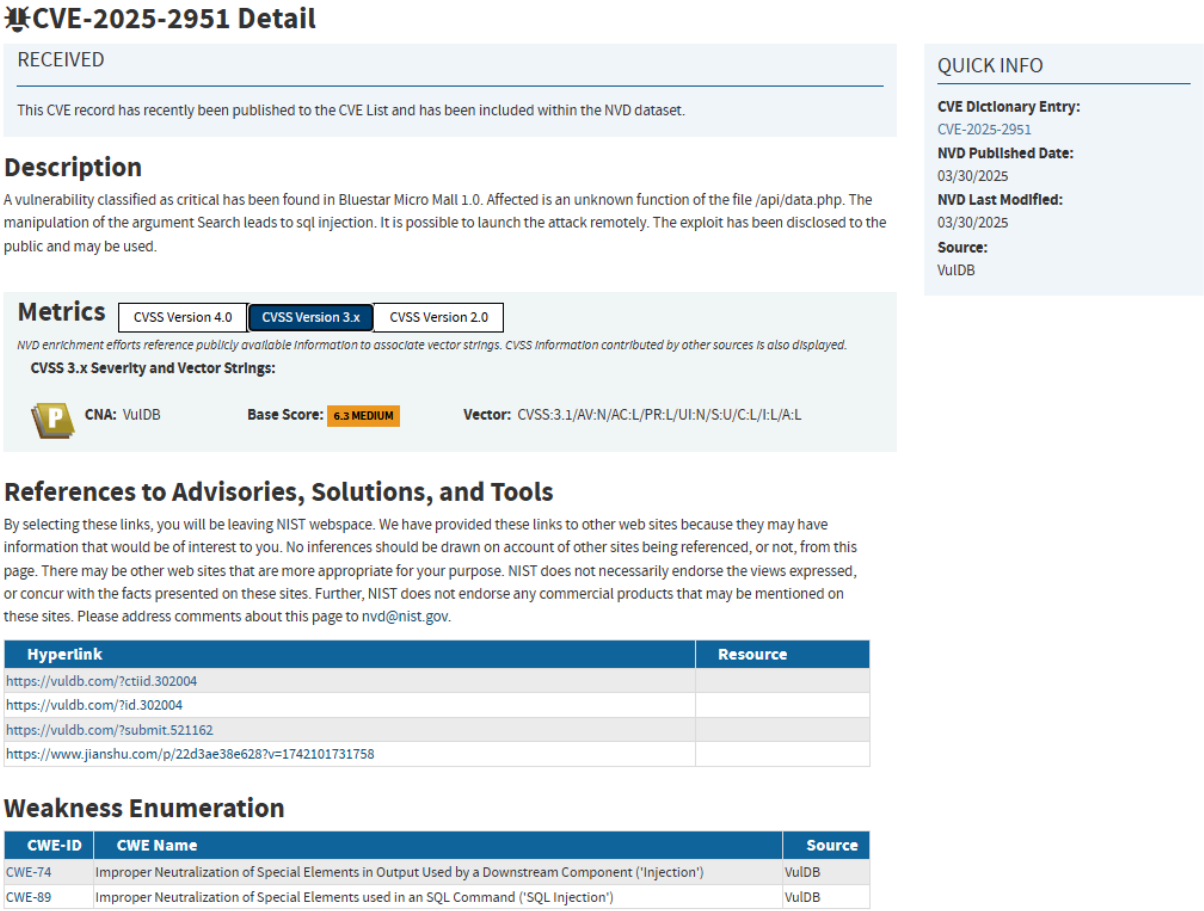
Show Matching CPE(s)

Figure 3: NIST Advisory for CVE-2025-2088 (SQL Injection Vulnerability)

Figure 3 displays a NIST Vulnerability Database entry for **CVE-2025-2088**, describing a SQL Injection vulnerability discovered in **PHPGurukul Pre-School Enrollment System <= v1.0**. The entry provides critical information including:

- **CVE Identifier**: *CVE-2025-2088*
- **Vulnerability Type**: *SQL Injection*
- **CVSS Score / Severity**: *CVSS 6.9 Medium* (as shown in the figure)
- **ProductName**: *Pre-School Enrollment System*
- **Version**: *<= 1.0*

- **Vendor**: *PHPGurukul*
- **Description**: Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber leads to sql injection.
- **Impact**: Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.
- **Mitigation**: Implement robust input validation and sanitization for the parameters (fullname, emailid, mobileNumber). Use parameterized queries or prepared statements to prevent SQL injection attacks.
- **DiscoveryDate**: 2025-03-13



CVE-2025-2951 Detail

RECEIVED

This CVE record has recently been published to the CVE List and has been included within the NVD dataset.

Description

A vulnerability classified as critical has been found in Bluestar Micro Mall 1.0. Affected is an unknown function of the file /api/data.php. The manipulation of the argument Search leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

QUICK INFO

CVE Dictionary Entry: CVE-2025-2951
NVD Published Date: 03/30/2025
NVD Last Modified: 03/30/2025
Source: VulDB

Metrics CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: VulDB **Base Score:** 6.3 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://vuldb.com/?ctiid.302004	
https://vuldb.com/?id.302004	
https://vuldb.com/?submit.521162	
https://www.jianshu.com/p/22d3ae38e628?v=1742101731758	

Weakness Enumeration

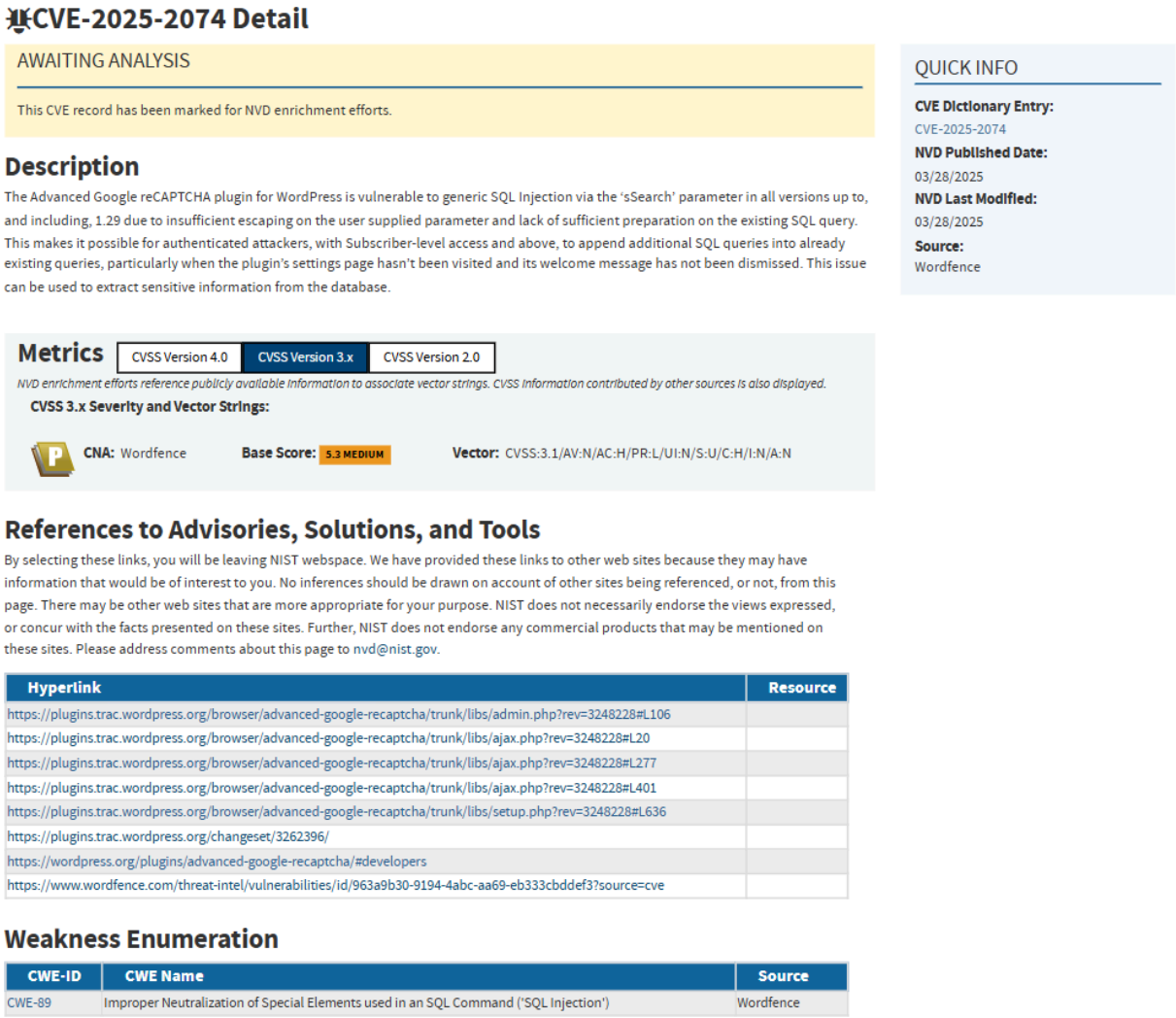
CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	VulDB
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	VulDB

Figure 4: NIST Advisory for CVE-2025-2951 (SQL Injection Vulnerability)

Figure 4 displays a NIST Vulnerability Database entry for **CVE-2025-2951**, describing a SQL Injection vulnerability discovered in **BlueStar Micro Mall v1.0**. The entry provides critical information including:

- **CVE Identifier:** *CVE-2025-2951*
- **Vulnerability Type:** *SQL Injection*
- **CVSS Score / Severity:** *CVSS 6.3 Medium (as shown in the figure)*
- **ProductName**: Micro Mall
- **Version**: *1.0*
- **Vendor**: *Bluestar*
- **Description**: Affected is an unknown function of the file /api/data.php. The manipulation of the argument Search leads to sql injection.
- **Impact**: Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.

- **Mitigation**: Implement strict input validation and sanitization for the "Search" parameter in the /api/data.php file. Use parameterized queries or prepared statements to prevent SQL injection attacks, and restrict database privileges to the minimum necessary.
- **DiscoveryDate**: 2025-03-30



CVE-2025-2074 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

The Advanced Google reCAPTCHA plugin for WordPress is vulnerable to generic SQL Injection via the 'sSearch' parameter in all versions up to, and including, 1.29 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries, particularly when the plugin's settings page hasn't been visited and its welcome message has not been dismissed. This issue can be used to extract sensitive information from the database.

QUICK INFO

CVE Dictionary Entry: CVE-2025-2074
NVD Published Date: 03/28/2025
NVD Last Modified: 03/28/2025
Source: Wordfence

Metrics CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Wordfence **Base Score:** 5.3 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://plugins.trac.wordpress.org/browser/advanced-google-recaptcha/trunk/libs/admin.php?rev=3248228#L106	
https://plugins.trac.wordpress.org/browser/advanced-google-recaptcha/trunk/libs/ajax.php?rev=3248228#L20	
https://plugins.trac.wordpress.org/browser/advanced-google-recaptcha/trunk/libs/ajax.php?rev=3248228#L277	
https://plugins.trac.wordpress.org/browser/advanced-google-recaptcha/trunk/libs/ajax.php?rev=3248228#L401	
https://plugins.trac.wordpress.org/browser/advanced-google-recaptcha/trunk/libs/setup.php?rev=3248228#L636	
https://plugins.trac.wordpress.org/changeset/3262396/	
https://wordpress.org/plugins/advanced-google-recaptcha/#developers	
https://www.wordfence.com/threat-intel/vulnerabilities/id/963a9b30-9194-4abc-aa69-eb333cbddef3?source=cve	

Weakness Enumeration

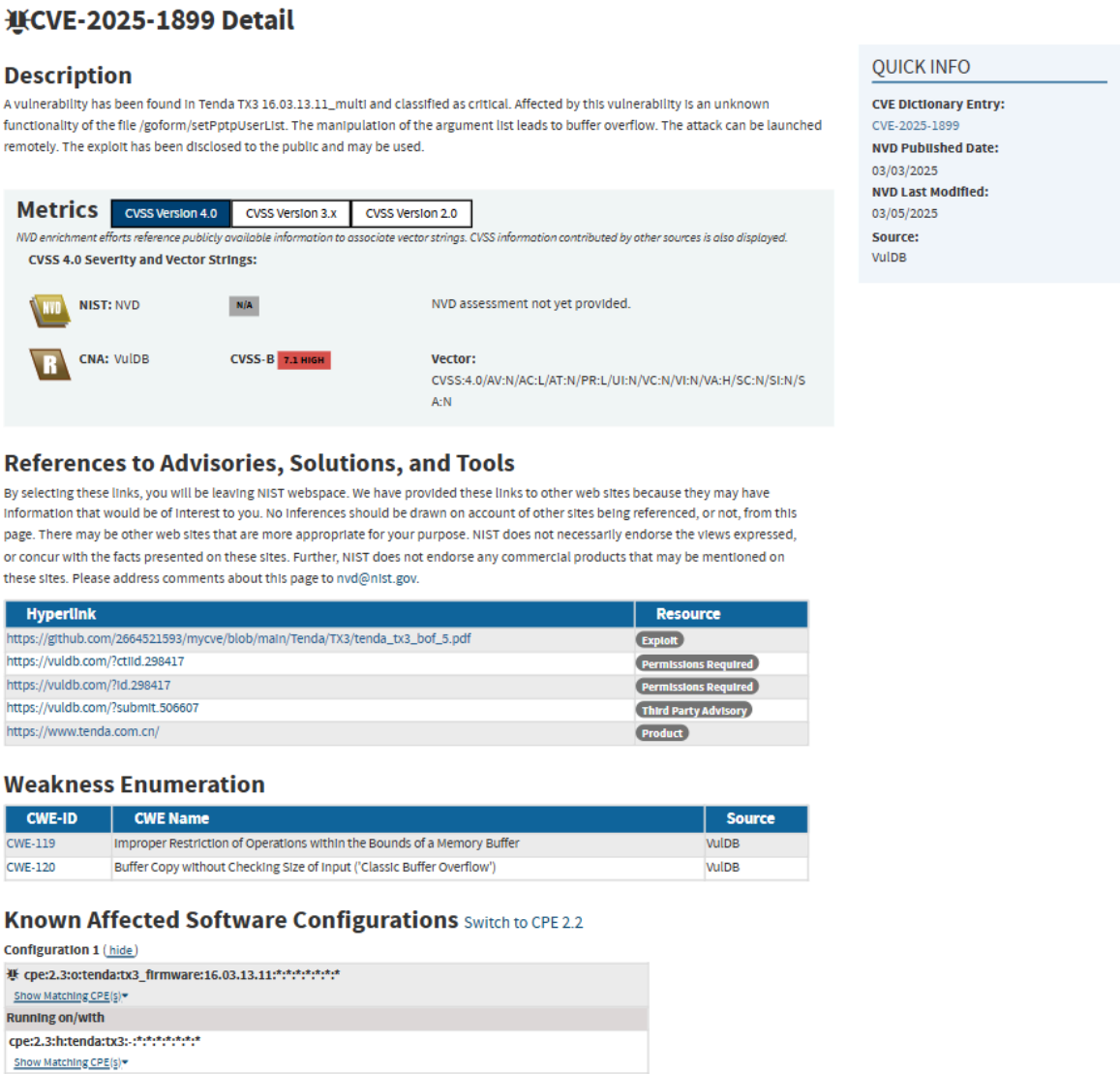
CWE-ID	CWE Name	Source
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Wordfence

Figure 5: NIST Advisory for CVE-2025-2074 (SQL Injection Vulnerability)

Figure 5 displays a NIST Vulnerability Database entry for **CVE-2025-2074**, describing a SQL Injection vulnerability discovered in the **Advanced Google reCAPTCHA plugin for WordPress v1.29**. The entry provides critical information including:

- **CVE Identifier:** *CVE-2025-2074*
- **Vulnerability Type:** *SQL Injection*
- **CVSS Score / Severity:** *CVSS 5.3 Medium (as shown in the figure)*
- **ProductName**: reCAPTCHA plugin for WordPress
- **Version**: *1.29*
- **Vendor**: *Google*
- **Description**: Due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query, 'sSearch'. This makes it possible for authenticated attackers to append additional SQL queries.
- **Impact**: Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to append additional SQL queries to existing ones, potentially extracting sensitive information from the database or manipulating its contents.

- **Mitigation**: Implement robust input sanitization and parameterized queries to securely handle the 'sSearch' parameter. Ensure that any user-supplied data is properly escaped and validated before use in SQL queries.
- **DiscoveryDate**: 2025-03-28



CVE-2025-1899 Detail

Description

A vulnerability has been found in Tenda TX3 16.03.13.11_multi and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.

QUICK INFO

CVE Dictionary Entry: CVE-2025-1899
NVD Published Date: 03/03/2025
NVD Last Modified: 03/05/2025
Source: VulDB

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD — N/A — NVD assessment not yet provided.

CNA: VulDB — **CVSS-B** 7.1 HIGH — **Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/2664521593/mycve/blob/main/Tenda/TX3/tenda_tx3_bof_5.pdf	Exploit
https://vuldb.com/?ctiid.298417	Permissions Required
https://vuldb.com/?id.298417	Permissions Required
https://vuldb.com/?submit.506607	Third Party Advisory
https://www.tenda.com.cn/	Product

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	VulDB
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	VulDB

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:tenda:tx3_firmware:16.03.13.11:*:*:*:*:*:*:*
Show Matching CPE(s)

Running on/with

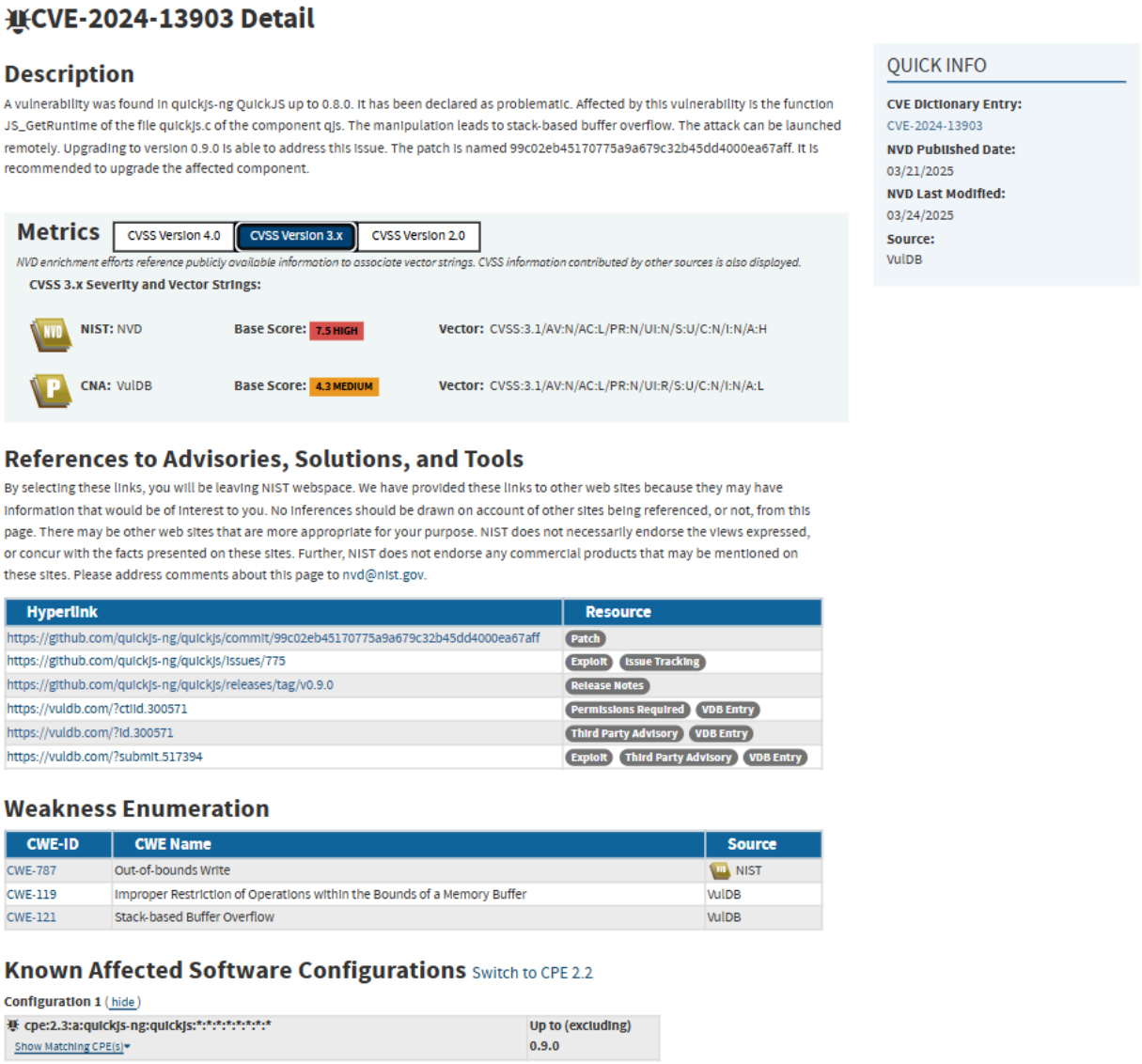
cpe:2.3:h:tenda:tx3:-:*:*:*:*:*:*:*
Show Matching CPE(s)

Figure 6: NIST Advisory for CVE-2025-1899 (Buffer Overflow Vulnerability)

Figure 6 highlights a **NIST Vulnerability Database** entry for **CVE-2025-1899**, describing a buffer overflow vulnerability in **Tenda TX3 V16.03.13.11_multi**. This advisory provides key data points, including:

- **CVE Identifier**: *CVE-2025-1899*
- **Vulnerability Type**: *Buffer Overflow*
- **Severity / CVSS Score**: *CVSS 7.1 High (as shown in the figure)*
- **ProductName**: TX3
- **Version**: *16.03.13.11_multi*
- **Vendor**: *Tenda*
- **Description**: Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow.
- **Impact**: Exploitation of this vulnerability may allow remote attackers to trigger a buffer overflow by manipulating the "list" parameter. This could result in memory corruption, system crashes, or potentially enable remote code execution, thereby compromising the affected device.

- **Mitigation**: Implement strict bounds checking and input validation on the "list" parameter in the /goform/setPptpUserList functionality. Ensure secure memory handling.
- **DiscoveryDate**: 2025-03-03



CVE-2024-13903 Detail

Description

A vulnerability was found in quickjs-ng QuickJS up to 0.8.0. It has been declared as problematic. Affected by this vulnerability is the function JS_GetRuntime of the file quickjs.c of the component qjs. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. Upgrading to version 0.9.0 is able to address this issue. The patch is named 99c02eb45170775a9a679c32b45dd4000ea67aff. It is recommended to upgrade the affected component.

QUICK INFO

CVE Dictionary Entry: CVE-2024-13903
NVD Published Date: 03/21/2025
NVD Last Modified: 03/24/2025
Source: VulDB

Metrics: CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	Base Score: 7.5 HIGH	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	
CNA: VulDB	Base Score: 4.3 MEDIUM	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L	

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/quickjs-ng/quickjs/commit/99c02eb45170775a9a679c32b45dd4000ea67aff	Patch
https://github.com/quickjs-ng/quickjs/issues/775	Exploit, Issue Tracking
https://github.com/quickjs-ng/quickjs/releases/tag/v0.9.0	Release Notes
https://vuldb.com/?ctiid.300571	Permissions Required, VDB Entry
https://vuldb.com/?id.300571	Third Party Advisory, VDB Entry
https://vuldb.com/?submit.517394	Exploit, Third Party Advisory, VDB Entry

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-787	Out-of-bounds Write	NIST
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	VulDB
CWE-121	Stack-based Buffer Overflow	VulDB

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

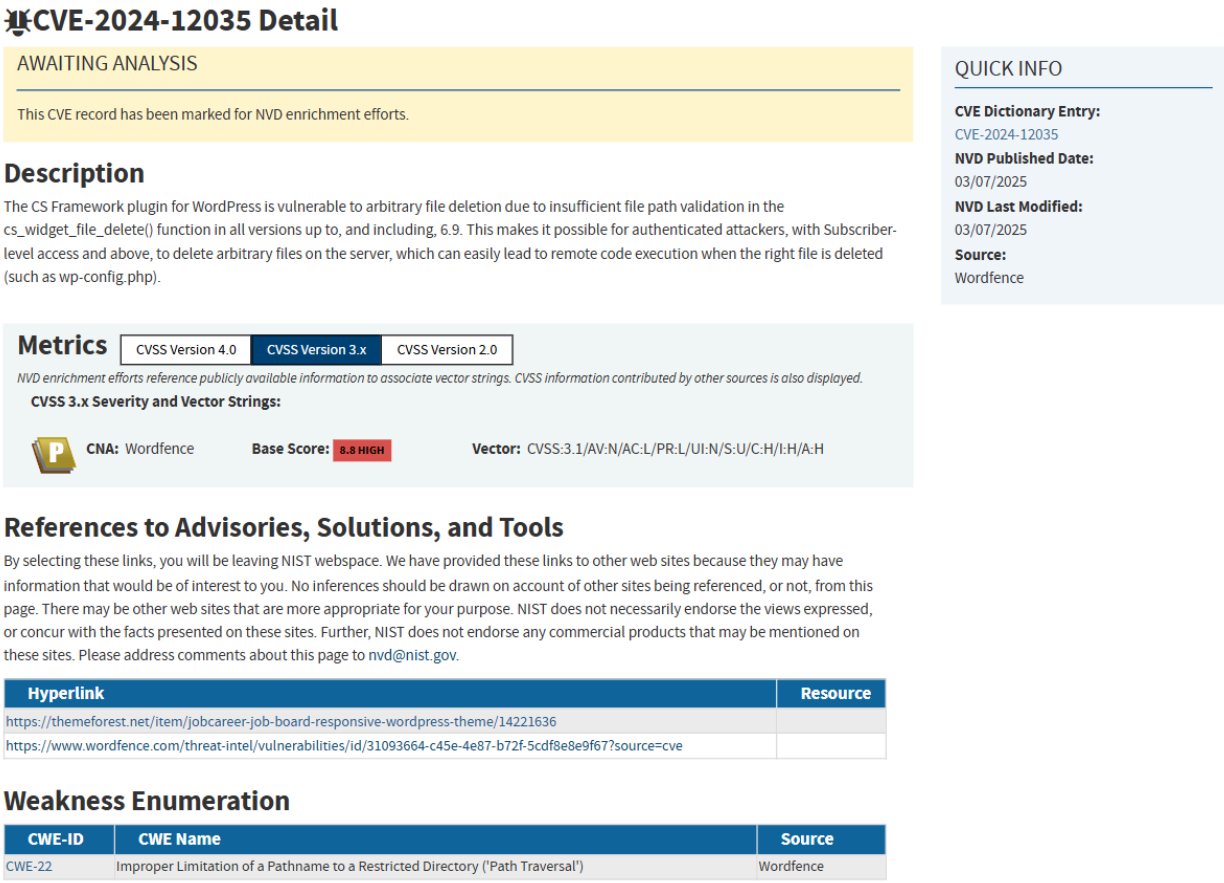
cpe:2.3:a:quickjs-ng:quickjs:*:*:*:*:*:*:*:* Show Matching CPE(s)	Up to (excluding) 0.9.0

Figure 7: NIST Advisory for CVE-2024-13903 (Buffer Overflow Vulnerability)

Figure 7 displays a NIST Vulnerability Database entry for **CVE-2024-13903**, describing a Buffer Overflow vulnerability discovered in **quickjs-ng <= v0.8.0**. The entry provides critical information including:

- **CVE Identifier:** *CVE-2024-13903*
- **Vulnerability Type:** *Buffer Overflow*
- **CVSS Score / Severity:** *CVSS 7.5 High (as shown in the figure)*
- ***ProductName***: *QuickJS*
- ***Version***: *<= 0.8.0*
- ***Vendor***: *quickjs-ng*
- **Description**: Affected by this vulnerability is the function JS_GetRuntime of the file quickjs.c of the component qjs. The manipulation leads to stack-based buffer overflow.
- **Impact**: Exploitation of this vulnerability allows remote attackers to trigger a stack-based buffer overflow within the JS_GetRuntime function, potentially leading to memory corruption, application crashes, and in the worst case, arbitrary code execution.

- **Mitigation**: Review and enforce secure coding practices, such as proper input validation and bounds checking, to prevent similar vulnerabilities.
- **DiscoveryDate**: 2025-03-21



CVE-2024-12035 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

The CS Framework plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cs_widget_file_delete() function in all versions up to, and including, 6.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).

QUICK INFO

CVE Dictionary Entry: CVE-2024-12035
NVD Published Date: 03/07/2025
NVD Last Modified: 03/07/2025
Source: Wordfence

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Wordfence **Base Score:** 8.8 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://themeforest.net/item/jobcareer-job-board-responsive-wordpress-theme/14221636	
https://www.wordfence.com/threat-intel/vulnerabilities/id/31093664-c45e-4e87-b72f-5cdf8e8e9f67?source=cve	

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Wordfence

Figure 8: NIST Advisory for CVE-2024-12035 (Remote Code Execution Vulnerability)

Figure 8 shows a **NIST Vulnerability Database** entry for **CVE-2024-12035**, describing a Remote Code Execution (RCE) vulnerability in the **CS Framework plugin for WordPress**. The advisory highlights:

- **CVE Identifier**: *CVE-2024-12035*
- **Vulnerability Type**: *Remote Code Execution*
- **CVSS Score / Severity**: *CVSS 8.8 High* (As indicated in the figure)
- ***ProductName***: *CS Framework for WordPress*
- ***Version***: *<= 6.9*
- ***Vendor***: *CS Framework*
- **Description**: The CS Framework plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cs_widget_file_delete() function.
- **Impact**: Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to delete arbitrary files on the server. By targeting critical files such as wp-config.php, attackers can achieve remote code execution and fully compromise the server.
- **Mitigation**: Enforce strict file path validation and restrict the file deletion functionality to only the intended and authorized directories. Additionally, ensure that file deletion operations are limited to users with the appropriate privileges.
- **DiscoveryDate**: 2025-03-07

CVE-2024-50310 Detail

Description

A vulnerability has been identified in SIMATIC CP 1543-1 V4.0 (6GK7543-1AX10-0XE0) (All versions >= V4.0.44 < V4.0.50). Affected devices do not properly handle authorization. This could allow an unauthenticated remote attacker to gain access to the filesystem.

QUICK INFO

CVE Dictionary Entry: CVE-2024-50310
NVD Published Date: 11/12/2024
NVD Last Modified: 11/13/2024
Source: Siemens AG

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 4.0 Severity and Vector Strings:

NIST: NVD	N/A		NVD assessment not yet provided.
CNA: Siemens AG	**CVSS-B** 8.7 HIGH		**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://cert-portal.siemens.com/productcert/html/ssa-654798.html	Patch, Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-863	Incorrect Authorization	Siemens AG

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

	From (including)	Up to (excluding)
cpe:2.3:o:siemens:simatic_cp_1543-1_firmware:*:*:*:*:*:*:*:* Show Matching CPE(s)	4.0.44	4.0.50
Running on/with		
cpe:2.3:h:siemens:simatic_cp_1543-1:-:*:*:*:*:*:*:* Show Matching CPE(s)		

Figure 9: NIST Advisory for CVE-2024-50310 (Information Disclosure Vulnerability)

Figure 9 presents a **NIST Vulnerability Database** entry for **CVE-2024-50310**, detailing an Information Disclosure vulnerability in **SIMATIC CP *1543-1 v4.0***. Key points from this advisory include:

- **CVE Identifier**: *CVE-2024-50310*
- **Vulnerability Type**: *Information Disclosure*
- **CVSS Score / Severity**: *CVSS 8.7 High* (As shown in the figure)
- **ProductName**: SIMATIC CP 1543-1
- **Version**: *4.0*
- **Vendor**: *Siemens*
- **Description**: Affected devices do not properly handle authorization.
- **Impact**: Exploitation of this vulnerability could allow unauthenticated remote attackers to bypass authorization mechanisms, gaining access to the filesystem. This may result in unauthorized data exposure, modification, or further system compromise.
- **Mitigation**: Enforce network segmentation and restrict remote access to critical systems to mitigate the risk of unauthorized access.
- **DiscoveryDate**: 2024-11-12

For the project's database requirements, I plan on capturing:

- **CVE ID**
- **Vulnerability Type**
- **CVSS Score**
- **ProductName**
- **Version**
- **Vendor**
- **Description**
- **Impact**
- **Mitigation**
- **DiscoveryDate**

This corresponds to Step A of the project, which involves gathering or generating real-world reports. Examining the data fields in the NIST entry provides a foundation for designing a more comprehensive database schema in Steps B and C, helping ensure all essential attributes are captured for effective vulnerability tracking and management.

Section B - User Views

Here we translate those source documents into stakeholder-focused views by defining SQL views that present the data in formats tailored to different audiences. These views will underpin the reporting requirements of our vulnerability-management system.

1. VulnerabilityOverviewDashboard

This view offers a clear, top-level overview of all known vulnerabilities, outlining essential details like CVE IDs, types, severity levels, impacted products, and when they were discovered. It helps decision-makers quickly gauge risk and prioritize actions, streamlining how security teams evaluate their organization's overall threat landscape.

```
CREATE VIEW VulnerabilityOverviewDashboard AS
SELECT
    VI.CVE_ID,
    VC.CategoryName AS Vulnerability_Type,
    VI.CVSS_Score,
    VI.Severity,
    P.ProductName AS Affected_Product,
    VI.DiscoveryDate
FROM VulnerabilityInstances VI
JOIN VulnerabilityCategories VC ON VI.CategoryID = VC.CategoryID
JOIN Product_Vulnerability PV ON VI.VulnerabilityInstanceID =
PV.VulnerabilityInstanceID
JOIN Products P ON PV.ProductID = P.ProductID
ORDER BY VI.DiscoveryDate DESC;
```

CVE_ID	Vulnerability_Type	CVSS_Score	Severity	Affected_Product	DiscoveryDate
CVE-2025-2951	SQL Injection	CVSS 6.3	Medium	Micro Mall	2025-03-30
CVE-2025-2074	SQL Injection	CVSS 5.3	Medium	reCAPTCHA plugin for WordPress	2025-03-28
CVE-2025-2699	Cross-Site Scripting	CVSS 5.1	Medium	ContentTools	2025-03-24
CVE-2024-13903	Buffer Overflow	CVSS 7.5	High	QuickJS	2025-03-21
CVE-2025-2088	SQL Injection	CVSS 6.9	Medium	Pre-School Enrollment System	2025-03-13
CVE-2024-12035	Remote Code Execution	CVSS 8.8	High	CS Framework for WordPress	2025-03-07
CVE-2025-2061	Cross-Site Scripting	CVSS 5.3	Medium	Online Ticket Reservation System	2025-03-06
CVE-2025-1899	Buffer Overflow	CVSS 7.1	High	TX3	2025-03-03
CVE-2024-50310	Information Disclosure	CVSS 8.7	High	SIMATIC CP 1543-1	2024-11-12

Figure 10: User view VulnerabilityOverviewDashboard

2. *DetailedVulnerabilityReport*

This view presents in-depth details for each vulnerability, covering technical summaries, potential impacts, and recommended mitigation steps. It's a critical tool for security analysts conducting detailed investigations to fully grasp each threat and develop targeted, effective response plans.

```
CREATE VIEW DetailedVulnerabilityReport AS
SELECT
    VI.VulnerabilityInstanceID,
    VI.CVE_ID,
    VC.CategoryName AS Vulnerability_Type,
    VI.CVSS_Score,
    VI.Severity,
    VI.Description,
    VI.Impact,
    VI.Mitigation,
    VI.DiscoveryDate,
    GROUP_CONCAT(P.ProductName SEPARATOR ', ') AS Affected_Products
FROM VulnerabilityInstances VI
JOIN VulnerabilityCategories VC ON VI.CategoryID = VC.CategoryID
JOIN Product_Vulnerability PV ON VI.VulnerabilityInstanceID =
PV.VulnerabilityInstanceID
JOIN Products P ON PV.ProductID = P.ProductID
GROUP BY VI.VulnerabilityInstanceID;
```

VulnerabilityInstanceID	CVE_ID	Vulnerability_Type	CVSS_Score	Severity
101	CVE-2025-2061	Cross-Site Scripting	CVSS 5.3	Medium
102	CVE-2025-2699	Cross-Site Scripting	CVSS 5.1	Medium
103	CVE-2025-2088	SQL Injection	CVSS 6.9	Medium
104	CVE-2025-2951	SQL Injection	CVSS 6.3	Medium
105	CVE-2025-2074	SQL Injection	CVSS 5.3	Medium
106	CVE-2025-1899	Buffer Overflow	CVSS 7.1	High
107	CVE-2024-13903	Buffer Overflow	CVSS 7.5	High
108	CVE-2024-12035	Remote Code Execution	CVSS 8.8	High
109	CVE-2024-50310	Information Disclosure	CVSS 8.7	High

Figure 11: User View DetailedVulnerabilityReport (1)

Description
This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name leads to cross site scripting.
Affected by this issue is some unknown functionality of the component Image Handler. The manipulation of the argument onload leads to cross site scripting.
Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber leads to sql injection.
Affected is an unknown function of the file /api/data.php. The manipulation of the argument Search leads to sql injection.
Due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query, "sSearch". This makes it possible for authenticated attackers to append additional SQL queries.
Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow.
Affected by this vulnerability is the function JS_GetRuntime of the file quickjs.c of the component qjs. The manipulation leads to stack-based buffer overflow.
The CS Framework plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cs_widget_file_delete() function.
Affected devices do not properly handle authorization.

Figure 12: User View DetailedVulnerabilityReport (2)

Impact
Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.
Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.
Exploitation of this vulnerability allows remote attackers to inject and execute malicious scripts in the context of a user's browser. This can lead to session hijacking, unauthorized actions, or theft of sensitive information.
Exploitation of this vulnerability allows remote attackers to trigger a stack-based buffer overflow within the JS_GetRuntime function, potentially leading to memory corruption, application crashes, and in the worst case, arbitrary code execution.
Exploitation of this vulnerability can allow remote attackers to inject and execute malicious scripts via the onload parameter, potentially leading to session hijacking, unauthorized data access, or client-side attacks such as phishing.
Exploitation of this vulnerability could allow unauthenticated remote attackers to bypass authorization mechanisms, gaining access to the filesystem. This may result in unauthorized data exposure, modification, or further system compromise.
Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to append additional SQL queries to existing ones, potentially extracting sensitive information from the database or manipulating its contents.
Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to delete arbitrary files on the server. By targeting critical files such as wp-config.php, attackers can achieve remote code execution and fully ...
Exploitation of this vulnerability may allow remote attackers to trigger a buffer overflow by manipulating the "list" parameter. This could result in memory corruption, system crashes, or potentially enable remote code execution, thereby compromising

Figure 13: User View DetailedVulnerabilityReport (3)

Mitigation	DiscoveryDate	Affected_Products
Implement robust input validation and sanitization for the parameters (fullname, emailid, mobileNumber). Use parameterized queries or prepared statemen...	2025-03-13	Pre-School Enrollment System
Implement strict input validation and sanitization for the "Search" parameter in the /api/data.php file. Use parameterized queries or prepared statements t...	2025-03-30	Micro Mall
Implement proper input validation and output encoding on the affected file (/passenger.php). Sanitize all user-supplied data to ensure special characters ...	2025-03-06	Online Ticket Reservation System
Review and enforce secure coding practices, such as proper input validation and bounds checking, to prevent similar vulnerabilities.	2025-03-21	QuickJS
Apply strict input validation and output encoding for the onload attribute in the Image Handler component. Additionally, review and patch the affected co...	2025-03-24	ContentTools
Enforce network segmentation and restrict remote access to critical systems to mitigate the risk of unauthorized access.	2024-11-12	SIMATIC CP 1543-1
Implement robust input sanitization and parameterized queries to securely handle the "sSearch" parameter. Ensure that any user-supplied data is properl...	2025-03-28	reCAPTCHA plugin for WordPress
Enforce strict file path validation and restrict the file deletion functionality to only the intended and authorized directories. Additionally, ensure that file del...	2025-03-07	CS Framework for WordPress
Implement strict bounds checking and input validation on the "list" parameter in the /goform/setPptpUserList functionality. Ensure secure memory handling.	2025-03-03	TX3

Figure 14:User View DetailedVulnerabilityReport (4)

3. *ProductVulnerabilityCorrelation*

This view connects each product with its associated vulnerabilities, showing the count per product alongside related CVE IDs. It enables product managers and IT teams to pinpoint high-risk assets, monitor evolving patterns, and strategically focus their efforts on patching and system enhancement where it matters most.

```
CREATE VIEW ProductVulnerabilityCorrelation AS
SELECT
    P.ProductName,
    P.Vendor,
    P.Version,
    COUNT(PV.VulnerabilityInstanceID) AS Vulnerability_Count,
    GROUP_CONCAT(VI.CVE_ID SEPARATOR ', ') AS Vulnerabilities
FROM Products P
JOIN Product_Vulnerability PV ON P.ProductID = PV.ProductID
JOIN VulnerabilityInstances VI ON PV.VulnerabilityInstanceID =
VI.VulnerabilityInstanceID
GROUP BY P.ProductID;
```

ProductName	Vendor	Version	Vulnerability_Count	Vulnerabilities
Online Ticket Reservation System	Code-projects	1.0	1	CVE-2025-2061
ContentTools	GetmeUK	<= 1.6.16	1	CVE-2025-2699
Pre-School Enrollment System	PHPGurukul	<= 1.0	1	CVE-2025-2088
Micro Mall	Bluestar	1.0	1	CVE-2025-2951
reCAPTCHA plugin for WordPress	Google	1.29	1	CVE-2025-2074
TX3	Tenda	16.03.13.11_multi	1	CVE-2025-1899
QuickJS	quickjs-ng	<= 0.8.0	1	CVE-2024-13903
CS Framework for WordPress	CS Framework	<= 6.9	1	CVE-2024-12035
SIMATIC CP 1543-1	Siemens	4.0	1	CVE-2024-50310

Figure 15: User View ProductVulnerabilityCorrelation

Section C - Database Schema

1. VulnerabilityCategories

CategoryID	CategoryName	Description
1	Cross-Site Scripting	Vulnerabilities allowing XSS attacks
2	SQL Injection	Vulnerabilities allowing SQL query manipulation
3	Buffer Overflow	Vulnerabilities causing memory errors
4	Remote Code Execution	Vulnerabilities that enable remote code execution
5	Information Disclosure	Vulnerabilities exposing sensitive data

Figure 16: VulnerabilityCategories Table

Purpose:
This table holds the distinct vulnerability types. Each category is defined only once and referenced by other tables.

Structure:
- **CategoryID** (Primary Key)
- **CategoryName**
- **Description**

Functional Dependency:
CategoryID → CategoryName, Description

Sample Tuple:
- (1, 'Cross-Site Scripting', 'Vulnerabilities allowing XSS attacks')

2. VulnerabilityInstances

VulnerabilityInstanceID	CVE_ID	CategoryID	CVSS_Score	Severity
101	CVE-2025-2061	1	CVSS 5.3	Medium
102	CVE-2025-2699	1	CVSS 5.1	Medium
103	CVE-2025-2088	2	CVSS 6.9	Medium
104	CVE-2025-2951	2	CVSS 6.3	Medium
105	CVE-2025-2074	2	CVSS 5.3	Medium
106	CVE-2025-1899	3	CVSS 7.1	High
107	CVE-2024-13903	3	CVSS 7.5	High
108	CVE-2024-12035	4	CVSS 8.8	High
109	CVE-2024-50310	5	CVSS 8.7	High

Figure 17: VulnerabilityInstances Table (1)

Description
This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name leads to cross site scripting.
Affected by this issue is some unknown functionality of the component Image Handler. The manipulation of the argument onload leads to cross site scripting.
Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber leads to sql injection.
Affected is an unknown function of the file /api/data.php. The manipulation of the argument Search leads to sql injection.
Due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query, "sSearch". This makes it possible for authenticated attackers to append additional SQL queries.
Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow.
Affected by this vulnerability is the function JS_GetRuntime of the file quickjs.c of the component qjs. The manipulation leads to stack-based buffer overflow.
The CS Framework plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cs_widget_file_delete() function.
Affected devices do not properly handle authorization.

Figure 18: VulnerabilityInstances Table (2)

Impact
Exploitation of this vulnerability allows remote attackers to inject and execute malicious scripts in the context of a user's browser. This can lead to session hijacking, unauthorized actions, or theft of sensitive information.
Exploitation of this vulnerability can allow remote attackers to inject and execute malicious scripts via the onload parameter, potentially leading to session hijacking, unauthorized data access, or client-side attacks such as phishing.
Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.
Exploitation of this SQL Injection vulnerability could allow remote attackers to execute unauthorized SQL queries, potentially leading to data leakage, modification, or deletion, and may compromise the integrity of the system.
Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to append additional SQL queries to existing ones, potentially extracting sensitive information from the database or manipulating its contents.
Exploitation of this vulnerability may allow remote attackers to trigger a buffer overflow by manipulating the "list" parameter. This could result in memory corruption, system crashes, or potentially enable remote code execution, thereby compromising
Exploitation of this vulnerability allows remote attackers to trigger a stack-based buffer overflow within the JS_GetRuntime function, potentially leading to memory corruption, application crashes, and in the worst case, arbitrary code execution.
Exploitation of this vulnerability enables authenticated attackers (with Subscriber-level access or higher) to delete arbitrary files on the server. By targeting critical files such as wp-config.php, attackers can achieve remote code execution and fully ...
Exploitation of this vulnerability could allow unauthenticated remote attackers to bypass authorization mechanisms, gaining access to the filesystem. This may result in unauthorized data exposure, modification, or further system compromise.

Figure 19: VulnerabilityInstances Table (3)

Mitigation	DiscoveryDate
Implement proper input validation and output encoding on the affected file (/passenger.php). Sanitize all user-supplied data to ensure special characters are handled safely, and apply secure coding practices to prevent script...	2025-03-06
Apply strict input validation and output encoding for the onload attribute in the Image Handler component. Additionally, review and patch the affected component in GetmeUK ContentTools.	2025-03-24
Implement robust input validation and sanitization for the parameters (fullname, emailid, mobileNumber). Use parameterized queries or prepared statements to prevent SQL injection attacks.	2025-03-13
Implement strict input validation and sanitization for the "Search" parameter in the /api/data.php file. Use parameterized queries or prepared statements to prevent SQL injection attacks, and restrict database privileges to th...	2025-03-30
Implement robust input sanitization and parameterized queries to securely handle the "sSearch" parameter. Ensure that any user-supplied data is properly escaped and validated before use in SQL queries.	2025-03-28
Implement strict bounds checking and input validation on the "list" parameter in the /goform/setPptpUserList functionality. Ensure secure memory handling.	2025-03-03
Review and enforce secure coding practices, such as proper input validation and bounds checking, to prevent similar vulnerabilities.	2025-03-21
Enforce strict file path validation and restrict the file deletion functionality to only the intended and authorized directories. Additionally, ensure that file deletion operations are limited to users with the appropriate privileges.	2025-03-07
Enforce network segmentation and restrict remote access to critical systems to mitigate the risk of unauthorized access.	2024-11-12

Figure 20: VulnerabilityInstances Table (4)

Purpose:
This table records each individual vulnerability instance, including detailed technical data. Each vulnerability is linked to a category via the CategoryID.

Structure:

- **VulnerabilityInstanceID** (Primary Key)
- **CVE_ID**
- **CategoryID** (Foreign Key referencing VulnerabilityCategories)
- **CVSS_Score**
- **Severity**
- **Description**
- **Impact**
- **Mitigation**
- **DiscoveryDate**

Functional Dependency:
VulnerabilityInstanceID → CVE_ID, CategoryID, CVSS_Score, Severity, Description, Impact, Mitigation, DiscoveryDate

Sample Tuple:

(101, 'CVE-2025-2061', 1, 'CVSS 5.3', 'Medium',
'This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name leads to cross site scripting.',
'Exploitation of this vulnerability allows remote attackers to inject and execute malicious scripts in the context of a user''s browser. This can lead to session hijacking, unauthorized actions, or theft of sensitive information.',

'Implement proper input validation and output encoding on the affected file (/passenger.php). Sanitize all user-supplied data to ensure special characters are handled safely, and apply secure coding practices to prevent script injection.',
'2025-03-06')

3. Products

ProductID	ProductName	Version	Vendor
1	Online Ticket Reservation System	1.0	Code-projects
2	ContentTools	<= 1.6.16	GetmeUK
3	Pre-School Enrollment System	<= 1.0	PHPGurukul
4	Micro Mall	1.0	Bluestar
5	reCAPTCHA plugin for WordPress	1.29	Google
6	TX3	16.03.13.11_multi	Tenda
7	QuickJS	<= 0.8.0	quickjs-ng
8	CS Framework for WordPress	<= 6.9	CS Framework
9	SIMATIC CP 1543-1	4.0	Siemens

Figure 21: Products Table

Purpose:
This table stores information about the products (or systems) that may be affected by vulnerabilities.

Structure:
- **ProductID** (Primary Key)
- **ProductName**
- **Version**
- **Vendor**

Functional Dependency:
ProductID → ProductName, Version, Vendor

Sample Tuple:
- (1, 'Online Ticket Reservation System', '1.0', 'Code-projects')

4. Product_Vulnerability

VulnerabilityInstanceID	ProductID
101	1
102	2
103	3
104	4
105	5
106	6
107	7
108	8
109	9

Figure 22: Product_Vulnerability Table

Purpose:
To represent the many-to-many relationship between vulnerabilities and products. A single vulnerability can affect multiple products, and a single product can have multiple vulnerabilities.

Structure:

- **VulnerabilityInstanceID** (Foreign Key referencing VulnerabilityInstances)
- **ProductID** (Foreign Key referencing Products)
- **Composite Primary Key:** (VulnerabilityInstanceID, ProductID)

Functional Dependency:
The combination (VulnerabilityInstanceID, ProductID) uniquely identifies each record.

Sample Tuple:

- (101, 1)