



脆弱性の識別、分類、評価

脆弱性の識別, 分類, 評価



脆弱性対応を適切に行うために...

■ 識別: 複数の脆弱性を扱う場面で誤解なく迅速に情報共有したい

CVE

■ 分類: 問題の性質を明確にし, 対応方法の迅速な理解につなげたい

CWE

■ 評価: 多数の脆弱性に対応する際の優先度付けをしたい

CVSS

脆弱性情報の例: JNVNU#92908006

<https://jvn.jp/vu/JNVNU92908006/>



公開日: 2023/06/01 最終更新日: 2023/06/01

JNVNU#92908006

三菱電機製MELSEC iQ-Rシリーズおよび iQ-Fシリーズにおける複数の脆弱性

概要

三菱電機製MELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびに EtherNet/IP設定ツールには、複数の脆弱性が存在します。

影響を受けるシステム

- MELSEC iQ-Rシリーズ EtherNet/IP ユニット
 - RJ71EIP91 すべてのバージョン
- RJ71EIP91用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCT-BD すべてのバージョン
- MELSEC iQ-Fシリーズ EtherNet/IP ユニット
 - FX5-ENET/IP すべてのバージョン
- FX5-ENET/IP用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCTFX5-BD すべてのバージョン


詳細情報

三菱電機株式会社が提供するMELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、次の複数の脆弱性が存在します。

- 不十分なパスワード強度 (**CWE-521**) - CVE-2023-2060
CVSS v3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 7.5
- ハードコードされたパスワードの使用 (**CWE-259**) - CVE-2023-2061
CVSS v3 CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 6.2

脆弱性情報の例: JNVNU#93149757 – 脆弱性の識別, CVE

<https://jvn.jp/vu/JNVNU93817405/>



公開日: 2023/06/01 最終更新日: 2023/06/01

JNVNU#92908006
三菱電機製MELSEC iQ-Rシリーズおよび iQ-Fシリーズにおける複数の脆弱性

概要
三菱電機製MELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、複数の脆弱性が存在します。

影響を受けるシステム

- MELSEC iQ-Rシリーズ EtherNet/IP ユニット
 - RJ71EIP91 すべてのバージョン
- RJ71EIP91用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCT-BD すべてのバージョン
- MELSEC iQ-Fシリーズ EtherNet/IP ユニット
 - FX5-ENET/IP すべてのバージョン
- FX5-ENET/IP用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCTFX5-BD すべてのバージョン


詳細情報
三菱電機株式会社が提供するMELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、次の複数の脆弱性が存在します。

- **不十分なパスワード強度 (CWE-521)** **CVE-2023-2060**
CVSS v3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 7.5
- **ハードコードされたパスワードの使用 (CWE-259)** - CVE-2023-2061
CVSS v3 CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 6.2

CVE ID
CVE-2023-2060

脆弱性情報の例: JNVNU#93149757 – 脆弱性の種類, CWE

<https://jvn.jp/vu/JNVNU93817405/>



公開日: 2023/06/01 最終更新日: 2023/06/01

JNVNU#92908006
三菱電機製MELSEC iQ-Rシリーズおよび iQ-Fシリーズにおける複数の脆弱性

概要

三菱電機製MELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびに EtherNet/IP設定ツールには、複数の脆弱性が存在します。

影響を受けるシステム

- MELSEC iQ-Rシリーズ EtherNet/IP ユニット
 - RJ71EIP91 すべてのバージョン
- RJ71EIP91用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCT-BD すべてのバージョン
- MELSEC iQ-Fシリーズ EtherNet/IP ユニット
 - FX5-ENET/IP すべてのバージョン
- FX5-ENET/IP用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCTFX5-BD すべてのバージョン

詳細情報

三菱電機株式会社が提供するMELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、次の複数の脆弱性が存在します。


- **不十分なパスワード強度 (CWE-521)** - CVE-2023-2060
CVSS v3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 7.5
- **ハードコードされたパスワードの使用 (CWE-259)** - CVE-2023-2061
CVSS v3 CVSS:3.1/AV:I/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 6.2

CWE-521

(Weak Password Requirements,
不十分なパスワード強度)

脆弱性情報の例: JNVNU#93149757 – 脆弱性の評価, CVSS

<https://jvn.jp/vu/JNVNU93817405/>



公開日: 2023/06/01 最終更新日: 2023/06/01

JNVNU#92908006
三菱電機製MELSEC iQ-Rシリーズおよび iQ-Fシリーズにおける複数の脆弱性

概要
三菱電機製MELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、複数の脆弱性が存在します。

影響を受けるシステム

- MELSEC iQ-Rシリーズ EtherNet/IP ユニット
 - RJ71EIP91 すべてのバージョン
- RJ71EIP91用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCT-BD すべてのバージョン
- MELSEC iQ-Fシリーズ EtherNet/IP ユニット
 - FX5-ENET/IP すべてのバージョン
- FX5-ENET/IP用 EtherNet/IP 設定ツール
 - SW1DNN-EIPCTFX5-BD すべてのバージョン

詳細情報
三菱電機株式会社が提供するMELSEC iQ-Rシリーズおよび iQ-FシリーズのEtherNet/IPユニットならびにEtherNet/IP設定ツールには、次の複数の脆弱性が存在します。

- 不十分なパスワード強度 (CWE-521)** - CVE-2023-2060
CVSS v3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N **基本値: 7.5**
- ハードコードされたパスワードの使用 (CWE-259)** - CVE-2023-2061
CVSS v3 CVSS:3.1/AV:I/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N **基本値: 6.2**

CVSS (Base Metrics)



脆弱性対応や他組織との情報交換のため、
対象とする脆弱性を特定する方法が欲しい



CVE

Common Vulnerability Enumeration

CVE Program



<https://www.cve.org/>

The screenshot shows the CVE Program website homepage. At the top, there's a navigation bar with links like 'About', 'Partner Information', 'Program Organization', 'Downloads', 'Resources & Support', and a 'Report/Request' button. Below the navigation bar, a welcome message states: 'Welcome to the new CVE Beta website! CVE List keyword search & downloads will be temporarily hosted on the old cve.mitre.org website until we complete the transition. Please use the CVE Program web forms for any comments or concerns.' The main heading is 'CVE® Program Mission', followed by the text: 'Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Currently, there are 179,418 CVE Records accessible via Download or Search'. A central graphic shows a globe with people icons around it, and text: 'The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of CVE Numbering Authorities (CNAs) and Roots.' Below this are two buttons: 'Learn More' and 'Become a Partner'. The page is divided into three main columns. The left column has 'Access' (List of Partners, CNA Rules, CVE Record Information, CVE Project on GitHub for Development) and 'Learn' (About CVE, Process, Program Organization, Terminology). The middle column has 'Report/Request' (Report vulnerability/Request CVE ID, Request CVE Record be published/updated, Report the use of a reserved CVE ID). The right column has 'News' (CVE List Download Formats Are Changing, The Value of Assigning CVEs, GE Healthcare Added as CVE Numbering Authority (CNA), Hitachi Vantara Added as CVE Numbering Authority (CNA)) and 'Events' (Automation Working Group (AWG) Meeting, CNA Coordination Working Group (CNACWG) Meeting, CVE Board Meeting, Quality Working Group (QWG) Meeting). At the bottom, there's a footer with 'Legal' (Terms of Use, Privacy Policy), 'Media' (News, Events, Sign up for e-newsletter), 'Social Media' (New CVE Records, CVE Announcement), and 'Contact' (CVE Program Support, CNA, CVE Website Support). A small disclaimer at the very bottom states: 'Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) & Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999-2022. The MITRE Corporation & CVE and the CVE logo are registered trademarks of The MITRE Corporation.'

- 1999年とあるワークショップでの提案が発祥
 - 複数の脆弱性データベース間の情報を関連付ける試み
- 米国政府の資金のもと、米国MITRE社のプロジェクトとして開始
- やがて脆弱性研究の興隆で業務逼迫
- 2016年あたりからは製品開発者(社)をCNAとする戦略へ

CVE情報の例: CVE-2023-2060



<https://www.cve.org/CVERecord?id=CVE-2023-2060>

CVE-2023-2060 PUBLISHED View JSON

Authentication bypass vulnerability in MELSEC iQ-R Series / iQ-F Series EtherNet/IP Modules

Important CVE JSON 5 Information

Assigner: Mitsubishi Electric Corporation

Published: 2023-06-02 **Updated:** 2023-06-02

Weak Password Requirements vulnerability in FTD function on Mitsubishi Electric Corporation MELSEC iQ-R

[About](#) [Partner Information](#) [Program Organization](#) [Downloads](#) [Resources & Support](#) [Re](#)

Product Status

Learn About the Versions Section

Vendor	Versions
Mitsubishi Electric Corporation	<i>Default Status:</i> unaffected <ul style="list-style-type: none">affected at all versions
Product	
MELSEC iQ-R Series EtherNet/IP module RJ71EIP91	
Vendor	Versions
Mitsubishi Electric Corporation	<i>Default Status:</i> unaffected <ul style="list-style-type: none">affected at all versions
Product	
MELSEC iQ-F Series EtherNet/IP module FX5-ENET/IP	

<https://cveawg.mitre.org/api/cve/CVE-2023-2060>

```
{
  "dataType": "CVE_RECORD",
  "dataVersion": "5.0",
  "cveMetadata": {
    "cveId": "CVE-2023-2060",
    "assignerOrgId": "e0f77b61-78fd-4786-b3fb-1ee347a748ad",
    "state": "PUBLISHED",
    "assignerShortName": "Mitsubishi",
    "dateReserved": "2023-04-14T08:43:59.259Z",
    "datePublished": "2023-06-02T04:02:32.377Z",
    "dateUpdated": "2023-06-02T04:02:32.377Z"
  },
  "containers": {
    "cna": {
      "affected": {
        "0": {
          "defaultStatus": "unaffected",
          "product": "MELSEC iQ-R Series EtherNet/IP module RJ71EIP91",
          "vendor": "Mitsubishi Electric Corporation",
          "versions": {
            "0": {
              "status": "affected",
              "version": "all versions"
            }
          }
        },
        "1": {
          "defaultStatus": "unaffected",
          "product": "MELSEC iQ-F Series EtherNet/IP module FX5-ENET/IP",
          "vendor": "Mitsubishi Electric Corporation",
          "versions": {
            "0": {
              "status": "affected",
              "version": "all versions"
            }
          }
        }
      }
    }
  }
}
```

■ 脆弱性の「種類」いろいろ

- 入力データ検証の不備
- SQLインジェクション
- 競合状態
- アクセス制御不備
- バッファオーバーフロー
-

脆弱性の種類を特定する
方法が欲しい



CWE

Common **W**eakness **E**numeration

CWE (Common Weakness Enumeration)



<https://cwe.mitre.org/>

**Common Weakness Enumeration**
A Community-Developed List of Software & Hardware Weakness Types

Top 25

Top HW CWE

New to CWE?
[Start here!](#)

ID Lookup: [Go](#)

[Home](#) | [About](#) | [CWE List](#) | [Mapping](#) | [Top-N Lists](#) | [Community](#) | [News](#) | [Search](#)

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

**2023 CWE Top 25 Most Dangerous Software Weaknesses** 

This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

[Top 25 List](#) | [Key Insights](#) | [Methodology](#)

CWE List Quick Access

Search CWE
ENHANCED BY Google

View CWE
[by Software Development](#)
[by Hardware Design](#)
[by Research Concepts](#)
[by Other Criteria](#)

Total Weaknesses: 933

Community Engagement

Hardware CWE Special Interest Group
[Join HW CWE SIG](#)

ICS/OT Special Interest Group
[Join ICS/OT SIG](#)

REST API Working Group
[Join REST API WG](#)

User Experience Working Group
[Join UE WG](#)

CWE/CAPEC Board
[Read meeting minutes](#)

Please see our [Guidelines for New Content Suggestions](#)
For other ways to get involved, [contact us](#)

CWE News

[News 2023 "CWE Top 25" Now Available!](#)

[News CWE Version 4.12 Now Available](#)

[News Enhancing Automotive Security with CWE](#)

[News Choose How You View CWE Weaknesses Using the New "Custom" Filter](#)

[News "New to CWE" Page Will Help You Get Started with CWE](#)

[More >>](#)

Page Last Updated: June 26, 2023

[Site Map](#) | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) |      

 Use of the Common Weakness Enumeration (CWE) and the associated references from this website are subject to the [Terms of Use](#). CWE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2008–2023, The MITRE Corporation. CWE, CWS, CWRAF, and the CWE logo are trademarks of The MITRE Corporation.





■ ソフトウェアやハードウェアの脆弱性分類一覧

■ 利点

- 脆弱性の理解を体系化できる
- 脆弱性アドバイザリにおける説明の簡素化
- 複数の脆弱性検査ツールにおける検査項目の共通化

■ 欠点

- 既存の分類に当てはまらない脆弱性を捉えられない

⇒ 定期的に CWE のバージョンアップが行われている

CWE View: Research Concepts (CWE-1000)



<https://cwe.mitre.org/data/definitions/1000.html>

**Common Weakness Enumeration**
A Community-Developed List of Software & Hardware Weakness Types



Home > CWE List > CWE- Individual Dictionary Definition (4.8)

ID Lookup: Go

Home | About | **CWE List** | Scoring | Mapping Guidance | Community | News | Search

CWE VIEW: Research Concepts

View ID: 1000
Type: Graph

Downloads: [Booklet](#) | [CSV](#) | [XML](#)

Objective

This view is intended to facilitate research into weaknesses, including their inter-dependencies, and can be leveraged to systematically identify theoretical gaps within CWE. It is mainly organized according to abstractions of behaviors instead of how they can be detected, where they appear in code, or when they are introduced in the development life cycle. By design, this view is expected to include every weakness within CWE.

Audience

Relationships

The following graph shows the tree-like relationships between weaknesses that exist at different levels of abstraction. At the highest level, categories and pillars exist to group weaknesses. Categories (which are not technically weaknesses) are special CWE entries used to group weaknesses that share a common characteristic. Pillars are weaknesses that are described in the most abstract fashion. Below these top-level entries are weaknesses are varying levels of abstraction. Classes are still very abstract, typically independent of any specific language or technology. Base level weaknesses are used to present a more specific type of weakness. A variant is a weakness that is described at a very low level of detail, typically limited to a specific language or technology. A chain is a set of weaknesses that must be reachable consecutively in order to produce an exploitable vulnerability. While a composite is a set of weaknesses that must all be present simultaneously in order to produce an exploitable vulnerability.

Show Details: ☐

Expand All | Collapse All | Filter View

1000 - Research Concepts

- Improper Access Control - (284)
- Improper Interaction Between Multiple Correctly-Behaving Entities - (435)
- Improper Control of a Resource Through its Lifetime - (664)
- Incorrect Calculation - (682)
- Insufficient Control Flow Management - (691)
- Protection Mechanism Failure - (693)
- Incorrect Comparison - (697)
- Improper Check or Handling of Exceptional Conditions - (703)
- Improper Neutralization - (707)
- Improper Adherence to Coding Standards - (710)
 - Use of Redundant Code - (1041)
 - Architecture with Number of Horizontal Layers Outside of Expected Range - (1044)
 - Invokable Control Element with Large Number of Outward Calls - (1048)
 - Insufficient Technical Documentation - (1059)
 - Insufficient Encapsulation - (1061)
 - Runtime Resource Management Control Element in a Component Built to Run on Application Servers - (1065)

CWE-79: Cross-site Scripting



<https://cwe.mitre.org/data/definitions/79.html>

CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.4) ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Weakness ID: 79
Abstraction: Base
Structure: Simple
Status: Stable

Presentation Filter:

Description

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

- Extended Description
- Alternate Terms
- Relationships
- Background Details
- Modes Of Introduction
- Applicable Platforms
- Common Consequences
- Likelihood Of Exploit
- Demonstrative Examples
- Observed Examples
- Potential Mitigations
- Weakness Ordinalities
- Detection Methods
- Memberships
- Notes
- Taxonomy Mappings
- Related Attack Patterns
- References
- Content History

Page Last Updated: March 15, 2021

Description
簡単な説明

Demonstrative Examples
コード例

Observed Examples
該当するCVE例

Potential Mitigations
対策の考え方

CWEの階層構造: CWE-77(Command Injection)の場合



<https://cwe.mitre.org/data/definitions/77.html>

CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77
Abstraction: Class
Structure: Simple

Status: Draft

Presentation Filter: Complete

Description

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.
2. The data is part of a string that is executed as a command by the application.
3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Command injection is a common problem with wrapper programs.

Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	74	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
ParentOf	78	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
ParentOf	88	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
ParentOf	624	624	Executable Regular Expression Error
ParentOf	917	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)

Relevant to the view "Architectural Concepts" (CWE-1008)

Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)

Relevant to the view "CISQ Data Protection Measures" (CWE-1340)

(1) タイトルと Description からこのCWE が意味するものを理解する。

(2) 他のCWEとの親子関係からより適切なCWEがあるか確認する。

CWE-74

CWE-77

CWE-78

CWE-88

CWE-624

CWE-917

TOP 25 Most Dangerous Software Errors



<https://cwe.mitre.org/top25/index.html>

2023年版 https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

The screenshot shows the MITRE CWE Top 25 Most Dangerous Software Weaknesses page for 2023. The page header includes the CWE logo, the title 'Common Weakness Enumeration', and a subtitle 'A Community-Developed List of Software & Hardware Weakness Types'. There are also icons for 'Top 25' and 'Top HW CWE', and a link 'New to CWE? Start here!'. The navigation bar includes links for Home, About, CWE List, Mapping, Top-N Lists, Community, News, and Search. The main content area is titled '2023 CWE Top 25 Most Dangerous Software Weaknesses' and includes a 'Share via:' button and a 'View in table format' button. The list of weaknesses is as follows:

Rank	Weakness	CVES in KEV	Rank Last Year
1	Out-of-bounds Write CWE-787	70	70
2	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-79	4	2
3	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-89	6	3
24	Incorrect Authorization CWE-863	0	28 (up 4) ▲
25	Incorrect Default Permissions CWE-276	0	20 (down 5) ▼

Page Last Updated: June 28, 2023

Site Map | Terms of Use | Privacy Policy | Contact Us | [Twitter](#) | [LinkedIn](#) | [YouTube](#) | [Facebook](#) | [M](#)

MITRE Use of the Common Weakness Enumeration (CWE) and the associated references from this website are subject to the Terms of Use. CWE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2006-2023, The MITRE Corporation. CWE, CWSS, CWRAP, and the CWE logo are trademarks of The MITRE Corporation.

HSSEDI

(中略)

最も危険な脆弱性トップ25

つまり.....
CVE情報から見た
「重点的に対策すべき脆弱性一覧」

2023年版は2022年と2021年に登録されたCVEに基づいて集計されている。

TOP 25 Most Dangerous Software Errors



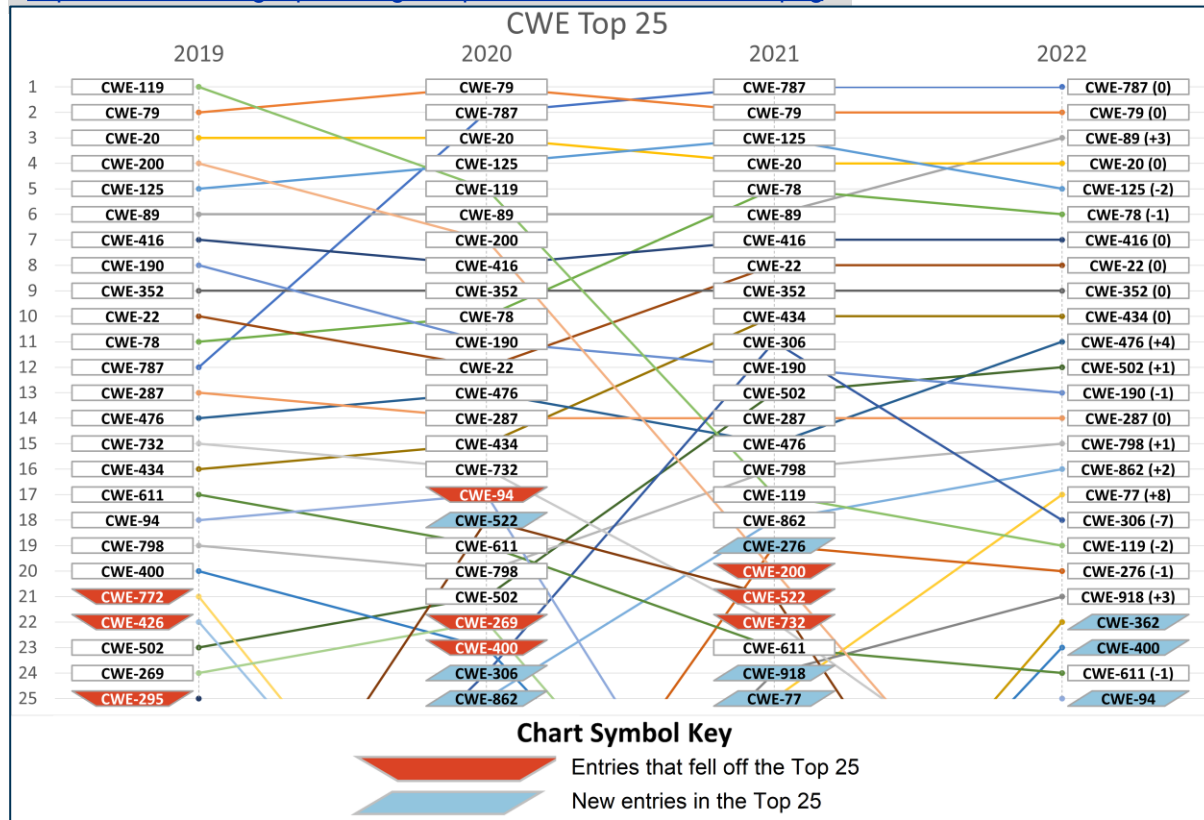
https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html#tableView

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2022
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	+3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	+1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorization	6.90	0	+5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	+1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialization of Untrusted Data	5.56	14	-3
16	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	4.95	4	+1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.75	7	+2
18	CWE-798	Use of Hard-coded Credentials	4.57	2	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	4.56	16	+2
20	CWE-306	Missing Authentication for Critical Function	3.78	8	-2
21	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.53	8	+1
22	CWE-269	Improper Privilege Management	3.31	5	+7
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6	+2
24	CWE-863	Incorrect Authorization	3.16	0	+4
25	CWE-276	Incorrect Default Permissions	3.16	0	-5

TOP 25 Most Dangerous Software Errors



<https://cwe.mitre.org/top25/images/top25-rank-trend-2019-2022.png>



"A second chart shows year-over-year changes from 2019 to 2022.

One can see the relative stability in the top 10 from 2021 to 2022, along with the steady rise of CWE-502: "Deserialization of Untrusted Data" over all four years."



■ 脆弱性評価の難しさ

- 評価者の主観に影響される
- 影響の大きさはシステム構成により異なる
- 脅威は時間の経過とともに変化する
- システム/サービスの重要度によって影響度は異なる (ビジネスインパクト)

誰もが利用できる汎用的
(vendor neutral) な指標が欲しい



CVSS

Common Vulnerability Scoring System

CVSS (Common Vulnerability Scoring System)



<https://www.first.org/cvss/>

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- CVSS v4.0 Public Preview
- Documentation & Resources
- CVSS v3.1 Documentation & Resources
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System SIG

Mission

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

Goals/Deliverables

CVSS is currently at version 3.1. Links on the left lead to CVSS version 3.1's specification and related resources.

A [self-paced on-line training course](#) is available for CVSS v3.1. It explains the standard without assuming any prior CVSS experience.

Current initiatives

The CVSS Special Interest Group (SIG) is proud to announce the official commencement of the **CVSS v4.0 Public Preview**. The latest information on CVSS v4.0 can be found [here](#).

The SIG is composed of representatives from a broad range of industry sectors, from banking and finance to technology and academia. Organizations and individuals interested in joining the SIG, or observing progress via the CVSS SIG mailing lists, should complete the Request to Join form below.

- 当初は米国政府組織(NIAC)が策定, その後 FIRST が管理団体に
- 10点満点で評価
- 最新版はv3.1
- 改訂版v4.0に向けて検討中



3つの観点で評価

- 基本値 (Base Metrics), 脆弱性自体の評価)
 - CIA(Confidentiality, Integrity, Availability)への影響
 - 遠隔, 同一セグメント, ローカル, 物理アクセス
 - 認証を突破する必要性
 - ユーザの関与の有無, など
- 現状値 (Temporal Metrics), 時間とともに変化する)
 - 攻撃コードの有無
 - ベンダが修正を提供しているかどうか
- 環境値 (Environmental Metrics), ユーザごとに異なる)
 - ユーザ固有の状況を考慮した脆弱性の評価

CVSS の例 (Base Score)



JPCERT/CCによる脆弱性分析結果

CVSS v3

CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L

基本値: 2.8 ▲

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	



脆弱性対応を適切に行うために...

- 識別: CVE を使って対象の脆弱性を明確にする
 - 複数の脆弱性を扱う場面で誤解なく迅速に情報共有
- 分類: CWE を使って脆弱性の種類を簡潔に示す
 - 問題の性質を明確にし, 対応方法の迅速な理解につなげる
- 評価: CVSS を使って脆弱性による影響を測る
 - 多数の脆弱性に対応する際の優先度付け

Thank you!

