

Vulnerability Countermeasure Information Database JVN iPedia Registration Status [2026 2nd Quarter (April – June)]

Vulnerability Countermeasure Information Database JVN iPedia Registration Status

This report provides an overview of the statistics and usage of vulnerability countermeasure information registered in JVN iPedia between April 1 and June 30, 2026.

Table of contents

1. 2026 2nd Quarter: Vulnerability Countermeasure Information Database JVN iPedia Registration Status	- 2 -
1-1. Vulnerabilities Registered in the 1st Quarter of 2026	- 2 -
2. Details on JVN iPedia Registered Data	- 3 -
2-1. Types of Vulnerabilities Reported.....	- 3 -
2-2. Severity of Vulnerabilities Reported	- 4 -
2-3. Types of Software Reported with Vulnerability.....	- 6 -
2-4. Products Reported with Vulnerability	- 7 -
3. Most Accessed Vulnerability Countermeasure Information.....	- 8 -

1. 2026 2nd Quarter: Vulnerability Countermeasure Information Database JVN iPedia Registration Status

The vulnerability countermeasure information database JVN iPedia (<https://jvndb.jvn.jp/en/>) is endeavoring to become a comprehensive vulnerability database where vulnerability countermeasure information is aggregated for easy access for IT users. JVN iPedia collects and/or translates the vulnerability countermeasure information published by 1) domestic software developers, 2) JVN^{(*)1}, a vulnerability countermeasure information portal run by JPCERT/CC and IPA, and 3) NVD^{(*)2}, a vulnerability database run by NIST^{(*)3}. JVN iPedia has been making vulnerability countermeasure information available to the public since April 25, 2007.

1-1. Vulnerabilities Registered in the 2nd Quarter of 2026

~JVN iPedia now stores 290,167 vulnerabilities~

The summary of the vulnerability countermeasure information registered to the Japanese version of JVN iPedia during the second quarter (April 1 to June 30) of 2026 is shown in the table below. As of the end of June 2026, **the total number of vulnerabilities stored in JVN iPedia is 290,167** (Table 1-1, Figure 1-1).

As for the JVN iPedia English version, the total number of vulnerabilities stored is 3,270 as shown in the lower half of Table 1-1.

**Table 1-1. Vulnerabilities Registered in JVN
iPedia in the 2nd Quarter of 2026**

	Information Source	Registered Cases	Cumulative Cases
Japanese Ver.	Domestic Software Developers	11	325
	JVN	109	17,588
	NVD	13,011	272,254
	Total	13,131	290,167
English Ver.	Domestic Software Developers	11	328
	JVN	55	2,942
	Total	66	3,270

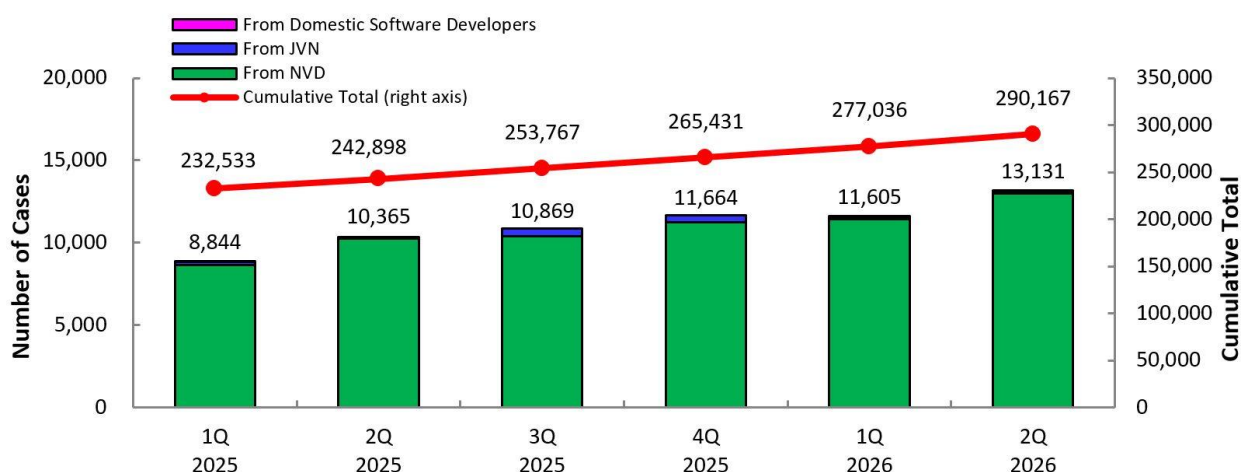


Figure 1-1. Quarterly Trends in Number of JVN iPedia Registered Vulnerabilities

^{(*)1} Japan Vulnerability Notes : A portal for vulnerability countermeasure information including information on vendor response to the reported vulnerabilities and security support. Operated in the collaboration of IPA and JPCERT/CC. <https://jvn.jp>

^{(*)2} National Vulnerability Database : A vulnerability database operated by NIST. <https://nvd.nist.gov>

^{(*)3} National Institute of Standards and Technology : A U.S federal agency that develops and promotes measurement, standards and technology. : <https://www.nist.gov>

2. Details on JVN iPedia Registered Data

2-1. Types of Vulnerabilities Reported

Figure 2-1 shows the number of vulnerabilities newly added to JVN iPedia during the second quarter (April 1 to June 30) of 2026, sorted by the CWE vulnerability types.

The most frequently reported vulnerability type in the first quarter is CWE-416 (Use After Free) with 749 cases, followed by CWE-79 (Cross-site Scripting) with 697 cases, CWE-20 (Improper Input Validation) with 445 cases, CWE-125 (Out-of-bounds Read) with 413 cases, and CWE-284 (Improper Access Control) with 398 cases. CWE-416 (Use After Free), the most commonly reported vulnerability type in this quarter, may allow attackers to exfiltrate or modify information and cause denial-of-service (DoS) conditions if successfully exploited.

Software developers need to make sure to mitigate vulnerability from the planning and design phase of software development. IPA provides tools and guidelines, such as “[Vulnerability Countermeasure Guide for Software Developers](#)”^{(*)4}, “[How to Secure Your Web-site](#)”^{(*)5}, and “[AppGoat](#)”^{(*)6}, a hands-on vulnerability learning tool, for website developers and operators to build secure websites.

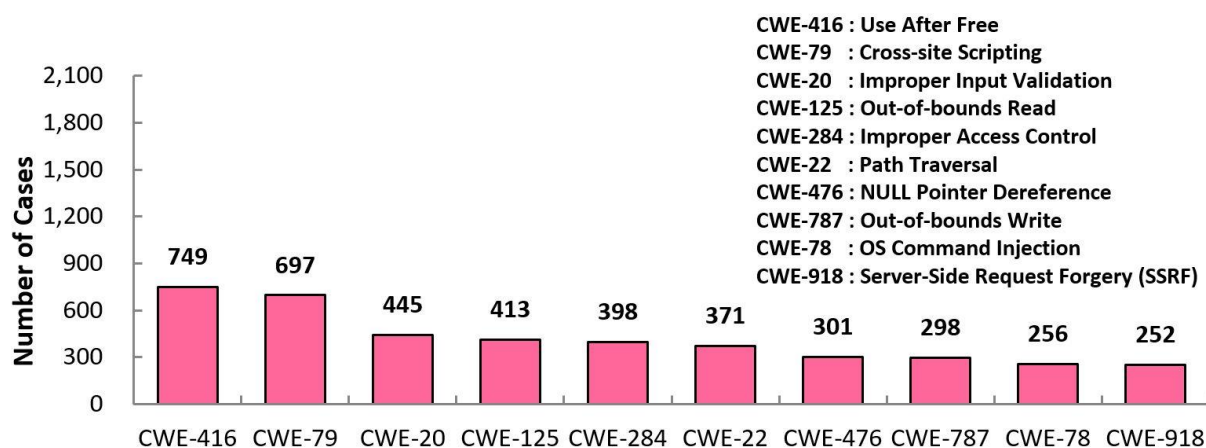


Figure 2-1. Types of Vulnerabilities Registered in 2026/2Q

^{(*)4}IPA : Vulnerability Countermeasure Guide for Software Developers (in Japanese only)
<https://www.ipa.go.jp/security/guide/vuln/forvendor.html>

^{(*)5}IPA : How to Secure Your Websites (latest version in Japanese only)
<https://www.ipa.go.jp/security/vuln/websecurity/about.html>

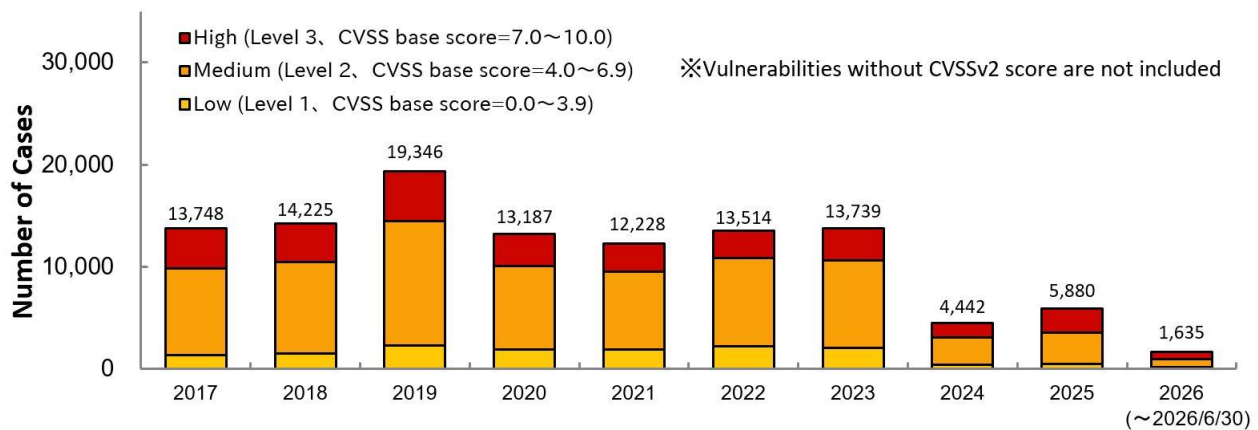
^{(*)6}IPA : AppGoat (in Japanese only)
<https://www.ipa.go.jp/security/vuln/appgoat/index.html>

2-2. Severity of Vulnerabilities Reported

Figure 2-2 shows the annual changes in vulnerabilities registered in JVN iPedia, categorized by severity level based on CVSS v2 scores.

Among the vulnerabilities registered in JVN iPedia in 2026, 44.7% are classified as Level 3 (7.0–10.0), 44.3% as Level 2 (4.0–6.9), and 11.0% as Level 1 (0.0–3.9). Overall, 89.0% are Level 2 or higher, indicating a high proportion of vulnerabilities that may lead to information exposure or data tampering.

The significant decrease in the number of CVSSv2 registrations in JVN iPedia since 2024 is due to the fact that CVSSv2 is no longer actively assessed by NVD, the information source for JVN iPedia^(*).



**Figure 2-2. Annual Changes in Severity of Registered Vulnerabilities (CVSSv2)
Over the Past 10 Years**

^(*)NIST : Retirement of CVSS v2
<https://nvd.nist.gov/general/news/retire-cvss-v2>

Figure 2-3 shows the annual changes in vulnerabilities registered in JVN iPedia, categorized by severity level based on CVSS v3 scores.

Among the vulnerabilities registered in JVN iPedia in 2026, 14.0% are classified as “Critical” (9.0–10.0), 42.5% as “High” (7.0–8.9), 41.3% as “Medium” (4.0–6.9), and 2.2% as “Low” (0.1–3.9).

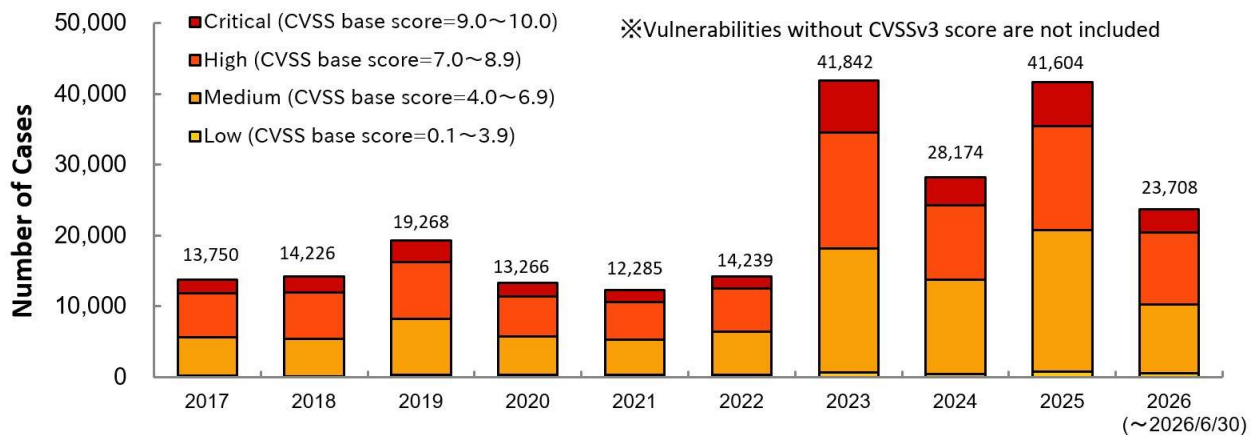


Figure 2-3. Annual Changes in Severity of Registered Vulnerabilities (CVSSv3) Over the Past 10 Years

To avoid the threats posed by the known vulnerabilities, both product developers and IT users should pay close attention to vulnerability disclosures and **update the software they use to a fixed version or apply a security patch** as soon as it becomes available. They can also check the JVN iPedia for new vulnerabilities that are published in RSS and XML formats^(*).

^(*)IPA : JVN iPedia Data Feeds (in Japanese only)
<https://jvndb.jvn.jp/ja/feed/>

2-3. Types of Software Reported with Vulnerability

Figure 2-4 shows the annual changes in the number of vulnerabilities registered in JVN iPedia, aggregated by software product type. Vulnerabilities related to applications account for the largest share in 2026, representing 74.0% (17,695 out of 23,912) of the total for that year.

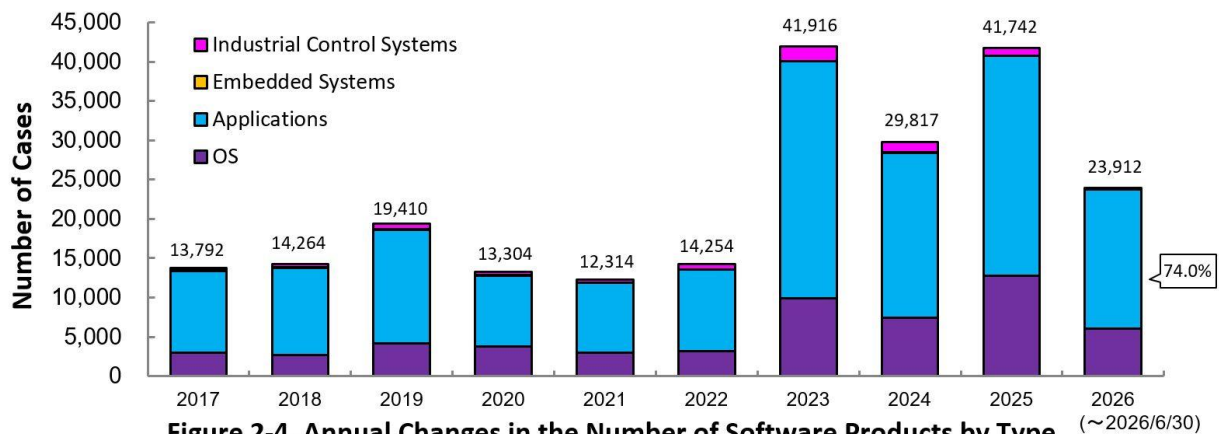


Figure 2-4. Annual Changes in the Number of Software Products by Type with Published Vulnerability Countermeasure Information Over the Past 10 Years

Figure 2-5 shows the annual changes in the number of vulnerabilities in industrial control systems (ICS), including those used in critical infrastructure, as registered in JVN iPedia.

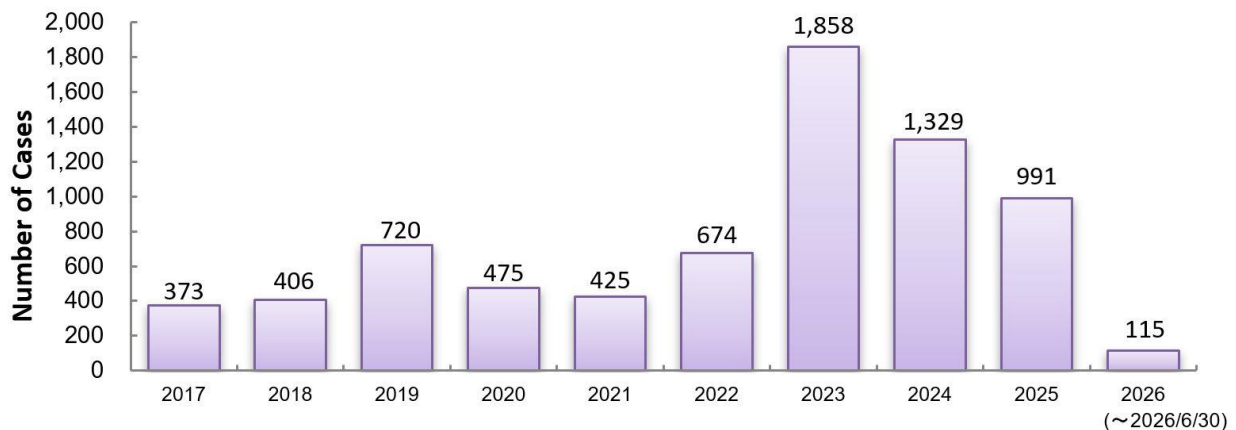


Figure 2-5. Number of Vulnerabilities Registered in JVN iPedia (ICS) Over the Past 10 Years

2-4. Products Reported with Vulnerability

Table 2-1 lists the top 20 software products with the highest number of vulnerabilities registered in JVN iPedia during the second quarter (April 1 to June 30) of 2026.

This quarter, Qualcomm components had the highest number of registered vulnerabilities, followed by the Linux kernel and Microsoft operating systems.

In addition to the products listed in the top 20 list, JVN iPedia provides a wide range of vulnerability countermeasure information. Software developers and users are encouraged to utilize JVN iPedia to quickly obtain information on vulnerabilities affecting the software used in their organizations and take appropriate action promptly^(*).

Table 2-1. Top 20 most registered software products vulnerability countermeasure information in JVN iPedia [Apr. – Jun. 2026]

Rank	Category	Product Name (Vendor)	Number of Vulnerabilities Registered
1	Firmware	Qualcomm component (Qualcomm)	5,183
2	OS	Linux Kernel (Linux)	1,514
3	OS	Microsoft Windows 11 (Microsoft)	1,121
4	Browser	Google Chrome (Google)	1,102
5	OS	Microsoft Windows 10 (Microsoft)	920
6	OS	Microsoft Windows Server 2022 (Microsoft)	451
7	AI Agent	OpenClaw (OpenClaw)	346
8	OS	Microsoft Windows Server 2025 (Microsoft)	295
9	OS	Microsoft Windows Server 2019 (Microsoft)	245
10	OS	Microsoft Windows Server 2016 (Microsoft)	205
11	OS	Microsoft Windows Server 2012 (Microsoft)	165
12	OS	Android (Google)	146
13	Browser	Mozilla Firefox (Mozilla Foundation)	140
14	Email Client	Mozilla Thunderbird (Mozilla Foundation)	124
15	OS	macOS (Apple)	118
16	OS	Red Hat Enterprise Linux (Red Hat)	85
17	UI	Open WebUI (Open WebUI)	81
17	Others	GitLab (GitLab.org)	81
19	OS	iOS (Apple)	74
19	OS	iPadOS (Apple)	74

^(*)IPA : Technical Watch - Daily Practice Guide (in Japanese only):
<https://www.ipa.go.jp/security/reports/technicalwatch/20150331.html>

3. Most Accessed Vulnerability Countermeasure Information

Table 3-1 lists the top 20 most frequently accessed vulnerability countermeasure information entries in JVN iPedia during the second quarter (April 1 to June 30) of 2026.

This quarter, all of the top 20 entries were vulnerability countermeasure information published on Japan Vulnerability Notes (JVN), a vulnerability countermeasure information portal.

**Table 3-1. Top 20 Most Accessed Vulnerability Countermeasure Information in JVN iPedia
[Apr. – Jun. 2026]**

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
1	JVNDB-2026-016006 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (in Japanese only)	-	10.0	May 18, 2026	23,133
2	JVNDB-2026-016098 Code Injection vulnerability in vm2 (vm2 project) (in Japanese only)	-	10.0	May 18, 2026	11,196
3	JVNDB-2026-016090 Multiple vulnerabilities in vm2 (vm2 project) (in Japanese only)	-	10.0	May 18, 2026	11,165
4	JVNDB-2026-016089 Code Injection vulnerability in vm2 (vm2 project) (in Japanese only)	-	10.0	May 18, 2026	11,104
5	JVNDB-2025-023591 Improper Access Control vulnerability in MetaCubeX Mihomo (in Japanese only)	-	6.5	Jan. 6, 2026	9,620
6	JVNDB-2026-009147 Vulnerability in Hitachi Infrastructure Analytics Advisor and Hitachi Ops Center Analyzer	-	8.2	Mar. 27, 2026	8,924
7	JVNDB-2026-016261 OS Command Injection vulnerability in PDF Export Module used in DHTMLX products (in Japanese only)	-	10.0	May 20, 2026	5,945
8	JVNDB-2026-015918 Information Disclosure vulnerability in Microsoft Authenticator (in Japanese only)	-	7.4	May 18, 2026	4,656
9	JVNDB-2025-001490 Vulnerability in 7-Zip (in Japanese only)	-	7.0	Feb. 13, 2026	4,599
10	JVNDB-2026-000050 Multiple vulnerabilities in Movable Type	-	9.8	Apr. 8, 2026	4,569
11	JVNDB-2026-000049 Multiple vulnerabilities in NEC Aterm series (NV26-001)	-	-	Apr. 3, 2026	4,439

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
12	JVNDB-2026-000051 SKYSEA Client View and SKYMEC IT Manager improper file access permission settings	-	7.8	Apr. 20, 2026	4,296
13	JVNDB-2026-000072 GUARDIANWALL MailSuite vulnerable to stack-based buffer overflow	-	9.8	May 13, 2026	3,992
14	JVNDB-2026-000073 Multiple vulnerabilities in ELECOM wireless LAN routers and access points (May 2026)	-	9.8	May 12, 2026	3,903
15	JVNDB-2026-000053 EmoCheck loads Dynamic Link Libraries insecurely	-	7.8	Apr. 10, 2026	3,876
16	JVNDB-2026-011159 Improper Authentication vulnerability in Multiple Products, Including Apache Tomcat from the Apache Software Foundation (in Japanese only)	-	9.1	Apr. 16, 2026	3,875
17	JVNDB-2026-000066 Open redirect vulnerability in multiple laser printers and MFPs which implement Ricoh Web Image Monitor	-	4.7	Apr. 30, 2026	3,626
18	JVNDB-2026-004072 Improper Check for Unusual or Exceptional Conditions vulnerability in axios from the axios project (in Japanese only)	-	7.5	Feb. 20, 2026	3,405
19	JVNDB-2026-000079 NEC Aterm series vulnerable to OS command injection (NV26-003)	-	6.8	May 25, 2026	3,359
20	JVNDB-2026-011174 HTTP Request/Response Smuggling vulnerability in Apache Tomcat from the Apache Software Foundation (in Japanese only)	-	7.5	Apr. 16, 2026	3,309

Table 3-2 shows the top 5 most accessed Vulnerability Countermeasure Information entries reported by domestic software developers.

**Table 3-2. Top 5 Most Accessed Vulnerabilities Reported by Domestic Product Developers
[Apr. – Jun. 2026]**

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
1	JVNDB-2026-009147 Vulnerability in Hitachi Infrastructure Analytics Advisor and Hitachi Ops Center Analyzer	-	8.2	Mar. 27, 2026	8,924
2	JVNDB-2026-016976 Security information for Hitachi Disk Array Systems	-	-	May 25, 2026	3,094
3	JVNDB-2026-010301 Multiple Vulnerabilities in JP1/IT Desktop Management 2 and JP1/NETM/DM	-	8.8	Apr. 8, 2026	2,886
4	JVNDB-2026-016983 Multiple Vulnerabilities in Cosminexus	-	-	May 27, 2026	2,675
5	JVNDB-2026-016981 Vulnerability in Hitachi Infrastructure Analytics Advisor, Hitachi Ops Center Analyzer and Hitachi Ops Center Analyzer viewpoint	-	4.6	May 27, 2026	2,653