Vulnerability Countermeasure Information Database

JVN iPedia Registration Status

[2026 3rd Quarter (July - September)]

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 July 1 and September 30, 2026.

Release Date: November 18, 2026
IPA IT Security Center

Table of contents

1. 2026 3rd Quarter: Vulnerability Countermeasure Information Database JVN iPedia Registration Status ..... - 2 -
1-1. Vulnerabilities Registered in the 3rd 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 3rd 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 3rd Quarter of 2026

～JVN iPedia now stores 310,240 vulnerabilities～

The summary of the vulnerability countermeasure information registered to the Japanese version of JVN iPedia during the third quarter (July 1 to September 30) of 2026 is shown in the table below. As of the end of September 2026, **the total number of vulnerabilities stored in JVN iPedia is 310,240** (Table 1-1, Figure 1-1).

As for the JVN iPedia English version, the total number of vulnerabilities stored is 3,346 as shown in the lower half of Table 1-1.

Table 1-1. Vulnerabilities Registered in JVN iPedia in the 3rd Quarter of 2026

	Information Source	Registered Cases	Cumulative Cases
Japanese Ver.	Domestic Software Developers	13	338
	JVN	147	17,735
	NVD	19,913	292,167
	Total	20,073	310,240
English Ver.	Domestic Software Developers	13	341
	JVN	63	3,005
	Total	76	3,346

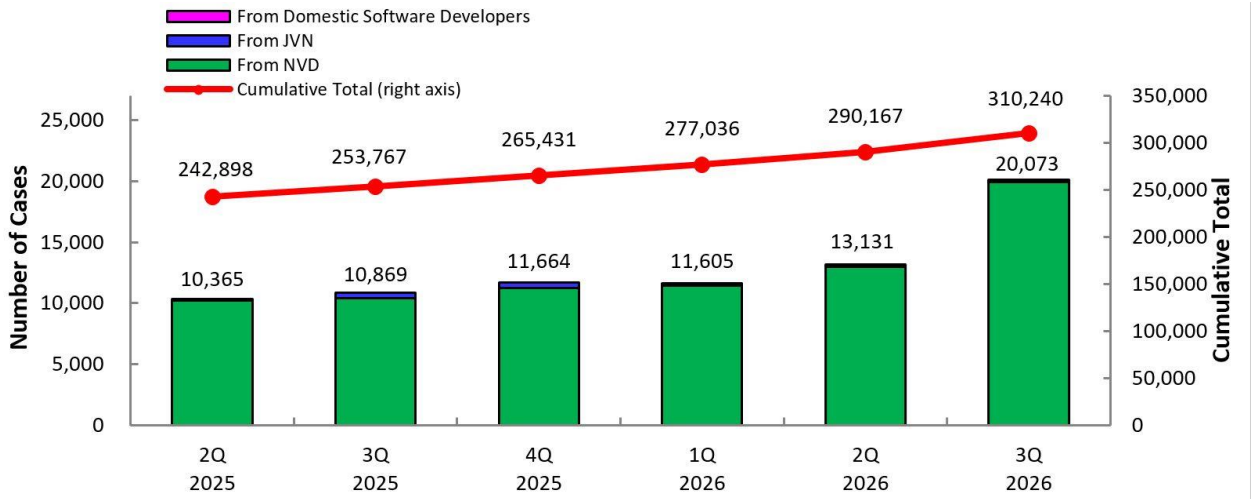


Figure 1-1. Quarterly Trends in Number of JVN iPedia Registered Vulnerabilities

[*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 third quarter (July 1 to September 30) of 2026, sorted by the CWE vulnerability types.

The most frequently reported vulnerability type in the third quarter is CWE-284 (Improper Access Control) with 1,580 cases, followed by CWE-416 (Use After Free) with 938 cases, CWE-122 (Heap-based Buffer Overflow) with 684 cases, CWE-125 (Out-of-bounds Read) with 602 cases, and CWE-20 (Improper Input Validation) with 522 cases. CWE-284 (Improper Access Control), 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 venerability learning tool, for website developers and operators to build secure websites.

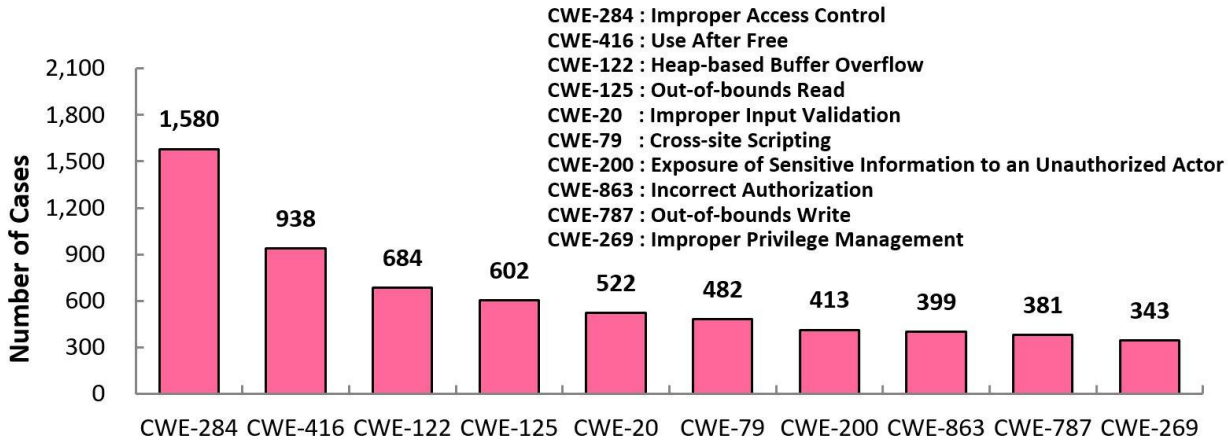


Figure 2-1. Types of Vulnerabilities Registered in 2026/3Q

(*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, 44.1% are classified as Level 3 (7.0-10.0), 44.3% as Level 2 (4.0-6.9), and 11.6% as Level 1 (0.0-3.9). Overall, 88.4% 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 [*7].

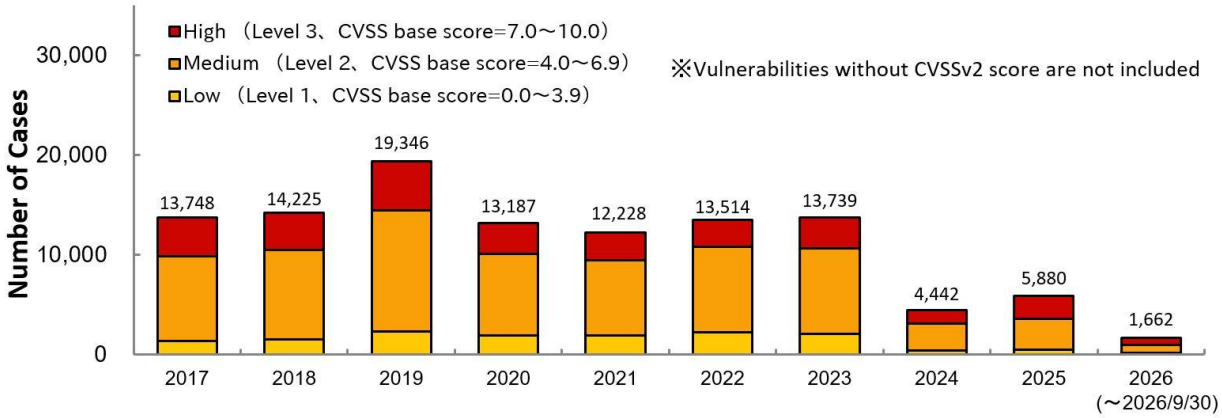


Figure 2-2. Annual Changes in Severity of Registered Vulnerabilities (CVSSv2) Over the Past 10 Years

[*7] 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, 13.6% are classified as “Critical” (9.0-10.0), 44.2% as “High” (7.0-8.9), 39.6% as “Medium” (4.0-6.9), and 2.5% as “Low” (0.1-3.9).

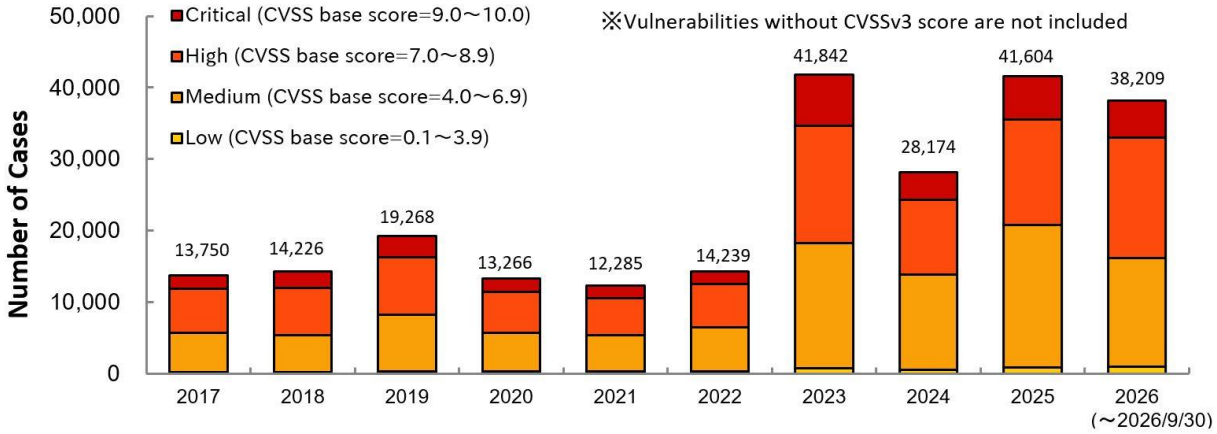


Figure 2-3. Annual Changes in Severity of Registered Vulnerabilities (CVSSv3) Over the Past 10 Years

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 [(*8)] .

[(*8)] 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 74.5% (28,703 out of 38,515) of the total for that year.

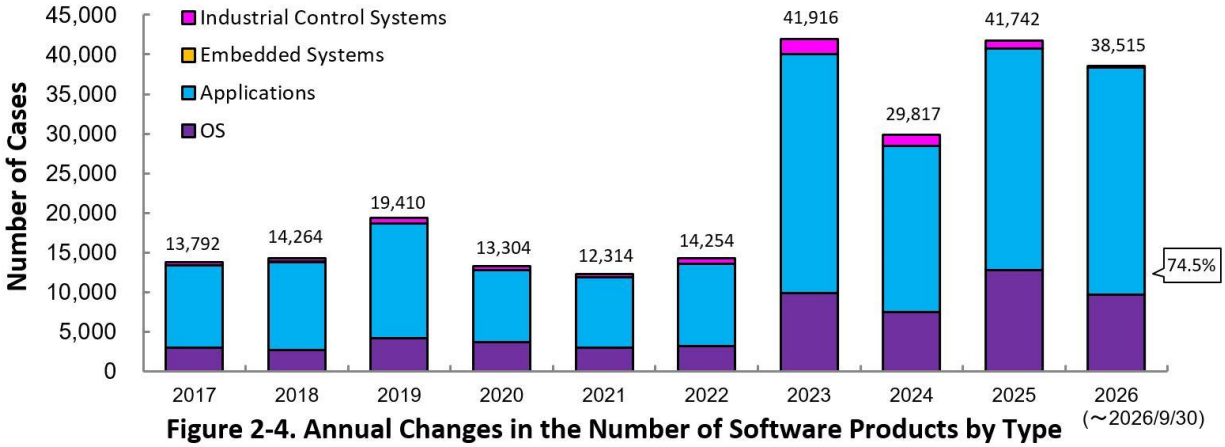


Figure 2-4. Annual Changes in the Number of Software Products by Type with Published Vulnerability Countermeasure Information Over the Past 10 Years

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.

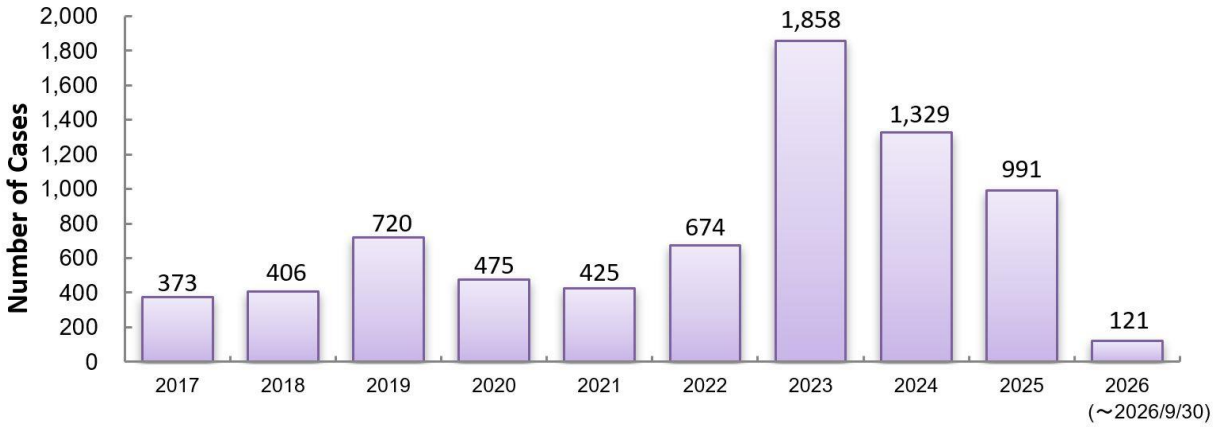


Figure 2-5. Number of Vulnerabilities Registered in JVN iPedia (ICS) Over the Past 10 Years

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 third quarter (July 1 to September 30) of 2026.

This quarter, Microsoft Windows 11 had the highest number of registered vulnerabilities, followed by Microsoft Windows 10 and Qualcomm components.

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 [(*9)] .

Table 2-1. Top 20 Most registered software products vulnerability countermeasure information in JVN iPedia [Jul. - Sep. 2026]

Rank	Category	Product Name（Vendor）	Number of Vulnerabilities Registered
1	OS	Microsoft Windows 11 (Microsoft)	4,278
2	OS	Microsoft Windows 10 (Microsoft)	4,029
3	Firmware	Qualcomm component (Qualcomm)	2,737
4	Browser	Google Chrome (Google)	1,590
5	OS	Microsoft Windows Server 2025 (Microsoft)	1,248
6	OS	Microsoft Windows Server 2022 (Microsoft)	1,128
7	OS	Microsoft Windows Server 2019 (Microsoft)	1,077
8	OS	Linux Kernel (Linux)	975
9	OS	Microsoft Windows Server 2016 (Microsoft)	937
10	OS	Microsoft Windows Server 2012 (Microsoft)	727
11	OS	macOS (Apple)	450
12	OS	iOS (Apple)	296
13	OS	iPadOS (Apple)	295
14	Business Software	Microsoft Office 2021 Long Term Servicing Channel Edition (Microsoft)	273
14	Business Software	Microsoft Office 2024 Long-Term Servicing Channel Edition (Microsoft)	273
16	Business Software	Microsoft 365 Apps (Microsoft)	272
17	Business Software	Microsoft Office 2019 (Microsoft)	266
18	Business Software	Microsoft Office 365 (Microsoft)	230
19	Browser	Android (Google)	223
20	OS	visionOS (Apple)	166

[(*9)] 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 third quarter (July 1 to September) 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 [Jul. - Sep. 2026]

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
1	**JVNDB-2026-000101** Drupal plugin "AI Agents" vulnerable to incorrect authorization	-	6.5	Jul. 21, 2026	9,684
2	**JVNDB-2026-000115** Sakura Editor vulnerable to OS command injection	-	7.8	Aug. 24, 2026	9,387
3	**JVNDB-2026-000085** Privilege escalation vulnerability in multiple RICOH and KONICA MINOLTA JAPAN printer drivers	-	7.8	Jun. 15, 2026	5,628
4	**JVNDB-2026-000092** Reflected cross-site scripting vulnerability in multiple laser printers and MFPs which implement Ricoh Web Image Monitor	-	6.1	Jun. 30, 2026	4,758
5	**JVNDB-2026-021994** Multiple vulnerabilities in Apache Tomcat（June 29, 2026）(in Japanese only)	-	-	Jul. 2, 2026	4,284
6	**JVNDB-2026-000099** Multiple vulnerabilities in TTSSH2 plugin of Tera Term	-	6.3	Jul. 16, 2026	4,041
7	**JVNDB-2026-000091** Seiko Solutions SkyBridge MB-A100/MB-A110 vulnerable to OS command injection	-	7.2	Jul. 1, 2026	4,002
8	**JVNDB-2026-000100** Vulnerability in certain IC chips of contactless IC card "FeliCa"	-	6.8	Jul. 21, 2026	3,933
9	**JVNDB-2026-000097** Multiple vulnerabilities in SKYSEA Client View and SKYMEC IT Manager	-	8.5	Aug. 24, 2026	3,898
10	**JVNDB-2026-000090** Multiple vulnerabilities in Fluentd	-	9.8	Jun. 29, 2026	3,890
11	**JVNDB-2026-000096** SEIKO EPSON printers and scanners Web Config vulnerable to cross-site request forgery	-	4.3	Jul. 7, 2026	3,691

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
12	**JVNDB-2026-000102** Ricoh printers and Multifunction Printers (MFPs) missing restriction on SSH port forwarding	-	5.8	Jul. 23, 2026	3,647
13	**JVNDB-2026-023874** Insufficient Technical Documentation vulnerability in Apache Tomcat from the Apache Software Foundation (in Japanese only)	-	9.1	Jul. 16, 2026	3,448
14	**JVNDB-2026-024104** Security information for Hitachi Disk Array Systems	-	-	Jul. 17, 2026	3,422
15	**JVNDB-2025-023591** MetaCubeX Mihomo vulnerable to Improper Access Control (in Japanese only)	-	6.5	Jan. 6, 2026	3,411
16	**JVNDB-2026-000095** Multiple vulnerabilities in the installer for Pupsman	-	7.8	Jul. 8, 2026	3,351
17	**JVNDB-2026-000109** Installer for LINE for Windows insecurely loads Dynamic Link Libraries	-	7.8	Aug. 10, 2026	3,190
18	**JVNDB-2024-011299** Multiple Microsoft products vulnerable to Denial of Service (DoS) (in Japanese only)	-	7.5	Oct. 28, 2024	3,150
19	**JVNDB-2026-000103** Multiple vulnerabilities in ELECOM wireless LAN routers and access points (July 2026)	-	7.2	Jul. 28, 2026	3,050
20	**JVNDB-2026-021658** Protection mechanism failure vulnerability in 7-Zip (in Japanese only)	-	3.3	July 1, 2026	3,012

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 [Jul. - Sep. 2026]

Rank	ID/Title	CVSSv2 Base Score	CVSSv3 Base Score	Publication Date	Access Count
1	**JVNDB-2026-024104** Security information for Hitachi Disk Array Systems	-	-	Jul. 17, 2026	3,422
2	**JVNDB-2026-029749** Security information for Hitachi Disk Array Systems	-	-	Aug. 24, 2026	2,091
3	**JVNDB-2026-026851** Vulnerability in Cosminexus HTTP Server and Hitachi Web Server	-	-	Aug. 5, 2026	2,009
4	**JVNDB-2026-018098** Security information for Hitachi Disk Array Systems	-	-	Jun. 4, 2026	1,947
5	**JVNDB-2026-026849** Vulnerability in Cosminexus HTTP Server	-	-	Aug. 5, 2026	1,943