# CVE-2024-41996

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2024-41996 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2024-08-26 06:15:04 UTC |
| **Updated** | 2026-05-12 12:17:03 UTC |
| **Description** | Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used. |

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**EPSS:** 0.006280000 probability, percentile 0.703590000 (date 2026-05-12)

**Problem Types:** CWE-295 | n/a | CWE-295 CWE-295 Improper Certificate Validation

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | ADP | DECLARED | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|---|---|---|---|
| CNA | Na | N/a | affected n/a |
| ADP | Diffie-hellman Key Exchange Project | Diffie-hellman Key Exchange | affected * custom |
| ADP | Siemens | RUGGEDCOM RST2428P | affected V3.3 custom |
| ADP | Siemens | SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCH328 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM324 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM328 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM332 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRH334 24 V DC 8xFO CC | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230 V AC 12xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230 V AC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 24 V DC 12xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 24 V DC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230 V AC 12xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230 V AC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SIDIS Prime | affected V4.0.800 custom |
| ADP | Siemens | SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem | affected * custom |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| cert-portal.siemens.com/productcert/html/ssa-089022.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com | |
| dheatattack.gitlab.io/details | cve@mitre.org | dheatattack.gitlab.io | |
| cert-portal.siemens.com/productcert/html/ssa-265688.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com | |
| gist.github.com/c0r0n3r/abccc14d4d96c0442f3a77fa5ca255d1 | cve@mitre.org | gist.github.com | |
| dheatattack.gitlab.io/faq | cve@mitre.org | dheatattack.gitlab.io | |
| cert-portal.siemens.com/productcert/html/ssa-485750.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com | |

| | | | |
|---|---|---|---|
| CVE Program record | CVE.ORG | www.cve.org | canon |
| NVD vulnerability detail | NVD | nvd.nist.gov | canon |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.



**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**