



# Unbounded exponent in decimal enables unauthenticated DoS

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-32686
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 15:16:05 UTC
<b>Updated</b>	2026-05-08 23:16:35 UTC

**Description** Uncontrolled Resource Consumption vulnerability in ericmj decimal allows unauthenticated remote Denial of Service. The d

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000710000 probability, percentile 0.215220000 (date 2026-05-08)

**Problem Types:** CWE-400 | CWE-400 CWE-400 Uncontrolled Resource Consumption

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Ericmj</a>	<a href="#">Decimal</a>	affected 0.1.0 3.0.0 semver
CNA	<a href="#">Ericmj</a>	<a href="#">Decimal</a>	affected bc11f4a2b6fb61fc1360a0ab4e79141bba918841_6a523f3a73b8c9974540e21c7aa88f1258bb35ae git

### References

Reference	Source	Link
<a href="https://github.com/ericmj/decimal/commit/6a523f3a73b8c9974540e21c7aa88f1258bb35ae">github.com/ericmj/decimal/commit/6a523f3a73b8c9974540e21c7aa88f1258bb35ae</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://github.com">github.com</a>
<a href="https://cna.erlef.org/cves/CVE-2026-32686.html">cna.erlef.org/cves/CVE-2026-32686.html</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://cna.erlef.org">cna.erlef.or</a>
<a href="https://github.com/ericmj/decimal/security/advisories/GHSA-rhv4-8758-jx7v">github.com/ericmj/decimal/security/advisories/GHSA-rhv4-8758-jx7v</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>
<a href="https://osv.dev/vulnerability/EEF-CVE-2026-32686">osv.dev/vulnerability/EEF-CVE-2026-32686</a>	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://osv.dev">osv.dev</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Peter Ullrich (en)

**CNA:** Eric Meadows-Jönsson (en)

**CNA:** José Valim (en)

**CNA:** Wojtek Mach (en)

**CNA:** Jonatan Männchen (en)

**CNA:** ruslandooa (en)

**CNA:** Matthew Johnston (en)

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)