



utils coreutils printenv Security Inspection Bypass via UTF-8 Enforcement

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

Summary

CVE	CVE-2026-35366
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 17:16:40 UTC
Updated	2026-05-04 18:52:42 UTC
Description	The printenv utility in utils coreutils fails to display environment variables containing invalid UTF-8 byte sequences. While F

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from security@ubuntu.com

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

EPSS: 0.000120000 probability, percentile 0.016120000 (date 2026-05-05)

Problem Types: CWE-754 | CWE-754 CWE-754: Improper Check for Unusual or Exceptional Conditions

Version	Source	Type	Score	Severity	Vector
3.1	security@ubuntu.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Utils	Coreutils	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Utils	Coreutils	affected 0.6.0 semver	Linux, Unix, macOS

References

Reference	Source	Link	Tags
github.com/uutils/coreutils/pull/9728	security@ubuntu.com	github.com	Issue Tracking, Patch
github.com/uutils/coreutils/releases/tag/0.6.0	security@ubuntu.com	github.com	Release Notes
github.com/uutils/coreutils/issues/9701	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Zellic (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