



Gotenberg: Chromium deny-list bypass via case-insensitive URL scheme

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

Summary

CVE	CVE-2026-27018
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 21:17:08 UTC
Updated	2026-04-01 14:24:21 UTC
Description	Gotenberg is an API for converting document formats. Prior to version 8.29.0, the fix introduced for CVE-2024-21527 can b

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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: 0.000160000 probability, percentile 0.037310000 (date 2026-04-02)

Problem Types: CWE-22 | CWE-918 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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
4.0	CNA	DECLARED	7.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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	Platforms
CNA	Gotenberg	Gotenberg	affected < 8.29.0	Not specified

References

Reference	Source	Link
github.com/gotenberg/gotenberg/security/advisories/GHSA-jjwv-57xh-xr6r	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.co
github.com/gotenberg/gotenberg/commit/06b2b2e10c52b58135edbf82e94d599eb...	security-advisories@github.com	github.co
github.com/gotenberg/gotenberg/commit/8625a4e899eb75e6fc46d28394334c7fd...	security-advisories@github.com	github.co
github.com/gotenberg/gotenberg/releases/tag/v8.29.0	security-advisories@github.com	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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](#).

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