text-generation-webui has a Path Traversal in load_prompt() — .txt file read without authentication

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

Summary

CVE	CVE-2026-35487
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 16:16:26 UTC
Updated	2026-04-09 18:46:11 UTC
Description	text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.3, an unauthenticated

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security-advisories@github.com

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

EPSS: 0.000680000 probability, percentile 0.209760000 (date 2026-04-15)

Problem Types: CWE-22 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oobabooga	Text Generation Web Ui	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oobabooga	Text-generation-webui	affected < 4.3	Not specified

References

Reference	Source	Link	Tags
github.com/oobabooga/text-generation-webui/security/advisories/GHSA-mfgg...	security-advisories@github.com	github.com	Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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