



# CISA manage.get.gov insecure portfolio administrative privileges

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

## Summary

<b>CVE</b>	CVE-2026-43510
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisa-cg
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 20:16:44 UTC
<b>Updated</b>	2026-05-07 20:32:03 UTC
<b>Description</b>	manage.get.gov is the .gov TLD registrar maintained by CISA. manage.get.gov allows an organization administrator to assi

## Risk And Classification

**Primary CVSS:** v4.0 7 HIGH from 9119a7d8-5eab-497f-8521-727c672e3725

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/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:** 0.000520000 probability, percentile 0.163100000 (date 2026-05-11)

**Problem Types:** CWE-266 | CWE-266 CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
4.0	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/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
4.0	CNA	DECLARED	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/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
3.1	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:H
3.1	CNA	DECLARED	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:H

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/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/MSG:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CISA	Manage.get.gov	affected 1.176.0 custom	Not specified
CNA	CISA	Manage.get.gov	unaffected 1.176.0	Not specified

### References

## References

Reference	Source
<a href="https://www.cve.org/CVERecord">www.cve.org/CVERecord</a>	9119a7d8-5eab-497f-8521-727c672e3725
<a href="https://github.com/cisagov/manage.get.gov/pull/4900">github.com/cisagov/manage.get.gov/pull/4900</a>	9119a7d8-5eab-497f-8521-727c672e3725
<a href="https://github.com/cisagov/manage.get.gov/releases/tag/v1.176.0">github.com/cisagov/manage.get.gov/releases/tag/v1.176.0</a>	9119a7d8-5eab-497f-8521-727c672e3725
<a href="https://github.com/cisagov/manage.get.gov/issues/4858">github.com/cisagov/manage.get.gov/issues/4858</a>	9119a7d8-5eab-497f-8521-727c672e3725
<a href="https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-121-01.json">raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-121-01.json</a>	9119a7d8-5eab-497f-8521-727c672e3725
<a href="https://github.com/cisagov/manage.get.gov/security/advisories/GHSA-6wrg-x3j6-x464">github.com/cisagov/manage.get.gov/security/advisories/GHSA-6wrg-x3j6-x464</a>	9119a7d8-5eab-497f-8521-727c672e3725
NVD vulnerability detail	NVD

## Vendor Comments And Credit

### Discovery Credit

**CNA:** bn-omran (@scofaild23) (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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)