



cPanel and WHM Authentication Bypass via Login Flow

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

Summary

CVE	CVE-2026-41940
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 16:16:25 UTC
Updated	2026-04-30 01:16:02 UTC
Description	cPanel and WHM versions after 11.40 contain an authentication bypass vulnerability in the login flow that allows unauthenti

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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	disclosure@vulncheck.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

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:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CPanel	CPanel	affected 11.110.0 11.110.0.97 semver	Not specified
CNA	CPanel	CPanel	affected 11.118.0 11.118.0.63 semver	Not specified
CNA	CPanel	CPanel	affected 11.126.0 11.126.0.54 semver	Not specified
CNA	CPanel	CPanel	affected 11.132.0 11.132.0.29 semver	Not specified
CNA	CPanel	CPanel	affected 11.134.0 11.134.0.20 semver	Not specified

CNA	CPanel	CPanel	affected 11.136.0 11.136.0.5 semver	Not specified
CNA	CPanel	CPanel	affected 11.86.0 11.86.0.41 semver	Not specified
CNA	CPanel	CPanel	affected 11.130.0 11.130.0.18 semver	Not specified
CNA	CPanel	WP Squared	affected 11.136.1 11.136.1.7 semver	Not specified
CNA	CPanel	WHM	affected 11.110.0 11.110.0.97 semver	Not specified
CNA	CPanel	WHM	affected 11.118.0 11.118.0.63 semver	Not specified
CNA	CPanel	WHM	affected 11.126.0 11.126.0.54 semver	Not specified
CNA	CPanel	WHM	affected 11.132.0 11.132.0.29 semver	Not specified
CNA	CPanel	WHM	affected 11.134.0 11.134.0.20 semver	Not specified
CNA	CPanel	WHM	affected 11.136.0 11.136.0.5 semver	Not specified
CNA	CPanel	WHM	affected 11.86.0 11.86.0.41 semver	Not specified
CNA	CPanel	WHM	affected 11.130.0 11.130.0.18 semver	Not specified

References

Reference	Source	Link
www.namecheap.com/status-updates/ongoing-critical-security-vulnerability-in-cpa...	disclosure@vulncheck.com	www.namecheap.com/status-updates/ongoing-critical-security-vulnerability-in-cpa...
github.com/watchtowrlabs/watchTower-vs-cPanel-WHM-AuthBypass-to-RCE.py	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com/watchtowrlabs/watchTower-vs-cPanel-WHM-AuthBypass-to-RCE.py
www.vulncheck.com/advisories/cpanel-and-whm-authentication-bypass-via-login-flow	disclosure@vulncheck.com	www.vulncheck.com/advisories/cpanel-and-whm-authentication-bypass-via-login-flow
support.cpanel.net/hc/en-us/articles/40073787579671-cPanel-WHM-Security-Update-0...	disclosure@vulncheck.com	support.cpanel.net/hc/en-us/articles/40073787579671-cPanel-WHM-Security-Update-0...
docs.wpsquared.com/changelogs/versions/changelog	disclosure@vulncheck.com	docs.wpsquared.com/changelogs/versions/changelog
docs.cpanel.net/release-notes/release-notes	disclosure@vulncheck.com	docs.cpanel.net/release-notes/release-notes
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

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