



# P10 Central Management Software 1.4.13 Denial of Service

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

## Summary

<b>CVE</b>	CVE-2018-25296
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-26 22:17:31 UTC
<b>Updated</b>	2026-04-26 22:17:31 UTC
<b>Description</b>	P10 Central Management Software 1.4.13 contains a buffer overflow vulnerability in the login password field that allows loc

## Risk And Classification

**Primary CVSS:** v4.0 6.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/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-120 | CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	P10	Central Management Software	affected 1.4.13	Not specified

### References

Reference	Source	Link
-----------	--------	------

<a href="http://www.vulncheck.com/advisories/p10-central-management-software-denial-of-service">www.vulncheck.com/advisories/p10-central-management-software-denial-of-service</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="http://www.vulncheck.com">www.vulncheck.com</a>
<a href="http://www.exploit-db.com/exploits/45207">www.exploit-db.com/exploits/45207</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
<a href="http://www.ambientweather.com">www.ambientweather.com</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="http://www.ambientweather.com">www.ambientweather.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Gionathan "John" Reale (en)

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

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