



# OCS Inventory NG Server Stored XSS via User-Agent

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

## Summary

<b>CVE</b>	CVE-2026-22675
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 22:16:20 UTC
<b>Updated</b>	2026-04-09 17:37:28 UTC
<b>Description</b>	OCS Inventory NG Server version 2.12.3 and prior contain a stored cross-site scripting vulnerability that allows unauthentic

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from disclosure@vulncheck.com

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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:** 0.000640000 probability, percentile 0.198760000 (date 2026-04-07)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	disclosure@vulncheck.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**Low**  
 User Interaction  
**Passive**  
 Confidentiality  
**None**  
 Integrity  
**None**  
 Availability  
**None**  
 Sub Conf.  
**Low**  
 Sub Integrity  
**Low**  
 Sub Availability  
**None**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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  
**Network**  
 Attack Complexity  
**Low**  
 Privileges Required  
**None**  
 User Interaction  
**Required**  
 Scope  
**Changed**  
 Confidentiality  
**Low**  
 Integrity  
**Low**  
 Availability  
**None**

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ocsinventory-ng	Ocs Inventory Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">OCS Inventory</a>	<a href="#">OCS Inventory NG Server</a>	affected 2.12.3 semver	Not specified
CNA	<a href="#">OCS Inventory</a>	<a href="#">OCS Inventory NG Server</a>	unaffected 78faf2ca8b897141ba4d337d75692ab8e405bd4e git	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/OCSInventory-NG/OCSInventory-Server/commit/78faf2ca8b897141ba4d337d75692ab8e405bd4e">github.com/OCSInventory-NG/OCSInventory-Server/commit/78faf2ca8b897141ba...</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>	Pa
<a href="https://www.vulncheck.com/advisories/ocs-inventory-ng-server-stored-xss-via-user-agent">www.vulncheck.com/advisories/ocs-inventory-ng-server-stored-xss-via-user-agent</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://www.vulncheck.com">www.vulncheck.com</a>	Th
<a href="https://github.com/OCSInventory-NG/OCSInventory-Server/pull/483">github.com/OCSInventory-NG/OCSInventory-Server/pull/483</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>	Is
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Alexandre Nesic (@\_atsika) at Quarkslab (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)