



# CVE-2020-28903

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

## Summary

<b>CVE</b>	CVE-2020-28903
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-24 13:15:00 UTC
<b>Updated</b>	2021-05-28 19:58:00 UTC
<b>Description</b>	Improper input validation in Nagios Fusion 4.1.8 and earlier allows a remote attacker with control over a fused server to inject

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Nagios</a>	<a href="#">Fusion</a>	All	All	All	All

## References

Reference	Source	Link	Tag
Nagios XI / Fusion Privilege Escalation / Cross Site Scripting / Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Skylight Cyber   13 Nagios Vulnerabilities, #7 will SHOCK you!	MISC	<a href="https://skylightcyber.com">skylightcyber.com</a>	
Nagios XI Change Log - Nagios	MISC	<a href="https://www.nagios.com">www.nagios.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[375647](#) Nagios XI And Nagios Fusion Multiple Vulnerabilities

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**