



# CVE-2018-18991

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-18991
<b>State</b>	PUBLIC
<b>Assigner</b>	ics-cert@hq.dhs.gov
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-04 21:29:00 UTC
<b>Updated</b>	2019-10-09 23:37:00 UTC
<b>Description</b>	Reflected cross-site scripting (non-persistent) in SCADA WebServer (Versions prior to 2.03.0001) could allow an attacker to

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Spidercontrol</a>	<a href="#">Scada Webserver</a>	All	All	All	All
Application	<a href="#">Spidercontrol</a>	<a href="#">Scada Webserver</a>	All	All	All	All

## References

Reference	Source	Link	Tags
SpiderControl SCADA WebServer   CISA	MISC	<a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>	Third Party Ac
SpiderControl SCADA WebServer CVE-2018-18991 Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Ac
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

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

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)