



# CVE-2018-1891

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

## Summary

<b>CVE</b>	CVE-2018-1891
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-17 16:29:00 UTC
<b>Updated</b>	2019-10-09 23:39:00 UTC
<b>Description</b>	IBM Security Guardium 10 and 10.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary J

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Security Guardium	All	All	All	All

## References

Reference	Source	Link
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/CVE-2018-1891">exchange.xforce.ibmcloud.com</a>
IBM Security Guardium CVE-2018-1891 Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com/bid/104444">www.securityfocus.com</a>
Security Bulletin: IBM Security Guardium is affected by a Cross-Site scripting vulnerabilities vulnerability	CONFIRM	<a href="https://www.ibm.com/support/ctgdoc/docid/I02548761.html">www.ibm.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org/CVE/nvd/cve/2018/1891">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-1891">nvd.nist.gov</a>

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)