



# CVE-2018-11065

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

## Summary

<b>CVE</b>	CVE-2018-11065
<b>State</b>	PUBLIC
<b>Assigner</b>	security_alert@emc.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-24 15:29:00 UTC
<b>Updated</b>	2019-10-09 23:33:00 UTC
<b>Description</b>	The WorkPoint component, which is embedded in all RSA Archer, versions 6.1.x, 6.2.x, 6.3.x prior to 6.3.0.7 and 6.4.x prior

## Risk And Classification

**Problem Types:** CWE-89

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsa	Archer	All	All	All	All
Application	Rsa	Archer	All	All	All	All

## References

### Reference

- Full Disclosure: DSA-2018-144: RSA Archer SQL Injection Vulnerability within embedded WorkPoint component
- RSA Archer Input Validation Flaw in Embedded WorkPoint Component Lets Remote Authenticated Users Inject SQL Commands - SecurityTr
- EMC RSA Archer GRC CVE-2018-11065 SQL Injection Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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)