



# CVE-2017-1710

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

## Summary

<b>CVE</b>	CVE-2017-1710
<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>	2017-11-13 23:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	A vulnerability in the Service Assistant GUI in IBM Storwize V7000 (2076) 8.1 could allow a remote attacker to perform a pr

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	ibm	Flashsystem V9000	-	All	All	All
Hardware	ibm	Flashsystem V9000	-	All	All	All
Operating System	ibm	Flashsystem V9000 Firmware	8.1	All	All	All
Operating System	ibm	Flashsystem V9000 Firmware	8.1	All	All	All
Hardware	ibm	San Volume Controller	-	All	All	All
Hardware	ibm	San Volume Controller	-	All	All	All
Operating System	ibm	San Volume Controller Firmware	8.1	All	All	All
Operating System	ibm	San Volume Controller Firmware	8.1	All	All	All
Hardware	ibm	Storwize V5000	-	All	All	All
Hardware	ibm	Storwize V5000	-	All	All	All
Operating System	ibm	Storwize V5000 Firmware	8.1	All	All	All
Operating System	ibm	Storwize V5000 Firmware	8.1	All	All	All
Hardware	ibm	Storwize V7000	-	All	All	All
Hardware	ibm	Storwize V7000	-	All	All	All
Operating System	ibm	Storwize V7000 Firmware	8.1	All	All	All
Operating System	ibm	Storwize V7000 Firmware	8.1	All	All	All

## References

### Reference

IBM X-Force Exchange

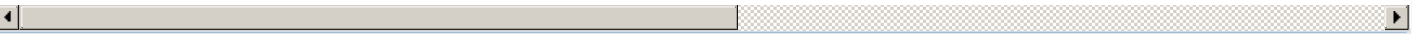
Multiple IBM Products CVE-2017-1710 Remote Privilege Escalation Vulnerability

Security Bulletin: Vulnerability in Service Assistant GUI affects SAN Volume Controller, Storwize family and FlashSystem V9000 products (CV

IBM Storwize Unspecified Flaw in Service Assistant GUI Lets Remote Users Gain Elevated Privileges - SecurityTracker

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.

© [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](#)

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