



CVE-2017-9631

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

Summary

CVE	CVE-2017-9631
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-07 17:29:00 UTC
Updated	2023-02-01 17:59:00 UTC
Description	A Null Pointer Dereference issue was discovered in Schneider Electric Wonderware Archedra Logger, versions 2017.426.2

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Wonderware Archedra Logger	All	All	All	All
Application	Schneider Electric	Wonderware Archedra Logger	All	All	All	All

References

Reference

- Schneider Wonderware Archedra Logger ICSA-17-187-04 Multiple Security Vulnerabilities
- Wonderware Information Server Flaws in Archedra Logger Component RPC Interface Let Remote Users Deny Service and Execute Arbitrary
- Schneider Electric Wonderware Archedra Logger | ICS-CERT
- AVEVA - Global Leader in Industrial Software
- 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](#).

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