

AVEVA PI Server: Denial of Service

Overview

On June 12, 2025, Broadcom published [CVE-2025-44019](#) detailing a denial of service vulnerability impacting AVEVA PI Server and PI Data Archive.

Affected Products and Versions

AVEVA PI Server 2018 SP3 Patch 6 and below

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2025-44019	7.1 (High)	5.4 (Medium)	AVEVA PI Server	Authentication Bypass (CWE-288)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

This vulnerability could enable an authenticated user to shut down necessary subsystems and cause a denial of service for the system.

Exploitation Status

GE Vernova has not yet observed or received any reports that Gas Power customer equipment has been compromised due to these vulnerabilities.

Remediation/Mitigation (Gas Power Customers)

This issue has been resolved in AVEVA PI Server 2018 SP3 Patch 7. Patch files can be obtained from the [OSISoft Customer Portal](#), searching for “AVEVA PI Server” and selecting Version 2018 SP3 Patch 7.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information. For Product Security issues or incident/vulnerability reporting: <https://www.gevernova.com/security>

Document History

Version	Release Date	Purpose
1.0	11/11/2025	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customers. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.