Windows Server: CVE-2026-41089

Overview

On May 12, 2026, Broadcom published CVE-2026-41089 detailing a buffer overflow vulnerability impacting Windows Server.

Affected Products and Versions

Control Server
OTArmor
Baseline Security Center
HA Domain Server

Windows Server 2012
Windows Server 2012 R2
Windows Server 2016 < 10.0.14393.9140
Windows Server 2019 < 10.0.17763.8755
Windows Server 2022 < 10.0.20348.5074
Windows Server 2022 23H2 < 10.0.24398.2330
Windows Server 2025 < 10.0.26100.32772

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
CVE-2026-41089	9.8 (Critical)	7.1 (High)	Windows Server	Stack-based Buffer Overflow (CWE-121)

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 in Windows Netlogon could enable an unauthorized user to send a malicious network request to a Windows Server installation configured to act as an Active Directory Domain Controller, potentially allowing the attacker to execute arbitrary code.

For Gas Power Controls customers, Domain Controllers are behind network segmentation, requiring an attacker to be on the local network to exploit this vulnerability. We utilize a secure-by-design, defense-in-depth strategy aiming to protect customer equipment from compromise.

Exploitation Status

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

Remediation/Mitigation (Gas Power Customers)

For Gas Power Patch Validation Program (PVP) customers, the latest monthly release includes the validated Windows Server security patches that address this vulnerability. For non-PVP customers, Microsoft has provided an update guide for affected Windows Server versions: Update Guide

For customers running Windows Server 2012, this update is only available from Microsoft via their Extended Security Update (ESU) program, which is not supported by Gas Power. We recommend that customers running Server 2012 contact their services representative for an upgrade to a supported Windows Server version.

Customers interested in the Patch Validation Program should also contact their services representative for future security updates should also contact their services representative.

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	6/24/2026	Initial Release

Disclaimer

GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Any rights and remedies arising out of or in connection with this Security Notice are subject to the applicable terms of a GE Vernova contract.