PRODUCT SECURITY ADVISORY

CARR-PSA-2025-02

September 22, 2025

VIESSMANN, Vitogate 300

Overview

This advisory covers notice by CISA of two vulnerabilities regarding Vitogate 300 product:

1. A vulnerability which affects the Viessmann Vitogate 300 device involves an OS command injection flaw leading to remote code execution.
2. An authentication bypass vulnerability exists in the Viessmann Vitogate 300 gateway device, allowing an attacker to gain full control over the device via frontend manipulation. The flaw enables an unauthorized user to bypass authentication by modifying HTML elements directly in the web browser.

Affected Products

Product	Version
Vitogate 300	VIESSMANN-Vitogate-300 versions prior to 3.1.0.1

Vulnerability Details

CVE ID	CVSS	Severity
CVE-2025-9494	Base Score: 8.5	High
CVE-2025-9495	Base Score: 8.7	High

CVE ID: CVE-2025-9494

CVSS v4.0 Base Score 8.5

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): The product constructs all or part of an OS command using

externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

CVE ID: CVE-2025-9495

CVSS v4.0 Base Score 8.7

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-602: Client-Side Enforcement of Server-Side Security: When the server relies on protection mechanisms placed on the client side, an attacker can modify the client-side behavior to bypass the protection mechanisms, resulting in potentially unexpected interactions between the client and server. The consequences will vary, depending on what the mechanisms are trying to protect.

Remediation

These vulnerabilities have been fixed with Vitogate 300 software version 3.1.0.1.

Customers are strongly encouraged to upgrade by downloading software version 3.1.0.1 or newer at the Vitogate 300 website.

About Carrier Global Product Cybersecurity

At Carrier, system and operational security is integral. The Product Security Incident Response Team (PSIRT) focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within Carrier products, offerings, solutions, components and/or services.

For more information about Global Product Security and PSIRT, please visit us at: https://www.corporate.carrier.com/product-security/

Or you may contact us at: productsecurity@carrier.com

Initial Publication Date	Last Publication Date
09/17/2025	09/17/2025