PRODUCT SECURITY ADVISORY

CARR-PSA-2024-03

September 10, 2024

Viessmann Vitogate 300

Overview

In September of 2023, security researchers published vulnerabilities impacting older versions of Viessmann Vitogate 300, an interface device that integrates Building Management Systems with Viessmann heating systems.

Viessmann Climate Solutions SE created a hotfix and communicated to customers in December of 2023.

An exploit for the two vulnerabilities was made public in March of 2024.

Viessmann Climate Solutions SE has since released a software update fully addressing the vulnerabilities.

The Integrated Viessmann Climate Solutions portfolio seamlessly connects products and systems via digital platforms and services. Viessmann Climate Solutions is part of Carrier Global Corporation, global leader in intelligent climate and energy solutions.

Affected Products

Product	Version
Viessmann Vitogate 300	Versions up to 2.1.3.0

Vulnerability Details

CVE ID	CVSS v4.0	Severity
CVE-2023-5222	Base Score 9.3	Critical
CVE-2023-5702	Base Score 7.1	High
CVE-2023-45852	Base Score 9.3	Critical

CVE ID: **CVE-2023-5222**

CVSS v4.0 Base Score 9.3 Critical AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-798 *Use of Hard-coded Credentials* affects the function isValidUser of the file /cgi-bin/vitogate.cgi of the component Web Management Interface. The manipulation leads to the use of hard coded-password.

CVE ID: **CVE-2023-5702**

CVSS v4.0 Base Score 7.1 High AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-425 *Direct Request ('Forced Browsing')* affects the file /cig-bin/. The manipulation leads to direct request.

CVE ID: **CVE-2023-45852**

CVSS v4.0 Base Score 9.3 Critical AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-77 *Improper Neutralization of Special elements used in a Command ('Command Injection')* in /cgi-bin/vitogate.cgi allows an unauthenticated attacker to bypass authentication and execute arbitrary commands via shell metacharacters in the ipaddr params JSON data for the put method.

Remediation

These vulnerabilities have been fixed with Vitogate 300 software version 3.0.0.0.

Customers are strongly encouraged to upgrade by downloading software version 3.0.0.0 at their 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. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

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 Published Date
09-10-2024	09-10-2024