Software Engineering Institute

CERT Coordination Center

Radware Cloud Web Application Firewall Vulnerable to Filter Bypass

Vulnerability Note VU#722229

Original Release Date: 2025-05-07 | Last Revised: 2025-05-07

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

Overview

The Radware Cloud Web Application Firewall is vulnerable to filter bypass by multiple means. The first is via specially crafted HTTP request and the second being insufficient validation of user-supplied input when processing a special character. An attacker with knowledge of these vulnerabilities can perform additional attacks without interference from the firewall.

Description

The Radware Cloud Web Application Firewall can be bypassed by means of a crafted HTTP request. If random data is included in the HTTP request body with a HTTP GET method, WAF protections may be bypassed. It should be noted that this evasion is only possible for those requests that use the HTTP GET method.

Another way the Radware Cloud WAF can be bypassed is if an attacker adds a special character to the request. The firewall fails to filter these requests and allows for various payloads to reach the underlying web application.

Impact

An attacker with knowledge of these vulnerabilities can bypass filtering. This allows malicious inputs to reach the underlying web application.

Solution

The vulnerabilities appear to be fixed, however Radware has not acknowledged the reporter's findings when they were initially disclosed.

Acknowledgements

Thanks to Oriol Gegundez for reporting this issue. This document was written by Kevin Stephens and Ben Koo.

Vendor Information

Filter by status: All

Filter by content: □ 📢 Additional information available

Sort by: Status

Expand all

Radware	Unknown

Other Information

CVE IDs:	CVE-2024-56523 CVE-2024-56524
API URL:	VINCE JSON | CSAF
Date Public:	2025-05-07
Date First Published:	2025-05-07

Date Last Updated: 2025-05-07 20:16 UTC

Document Revision: 1

Sponsored by CISA.

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact CERT/CC

☎ 412-268-5800
✉ cert@cert.org