Security Advisory 2026-05

Jun 11, 2026 · VULNERABILITY/STORED XSS SEVERITY/MEDIUM CVSS/5.6

Summary	Stored XSS using artifacts
Advisory Number	2026-05
Discovery Date	19 MAR 2026
Patch Release Date	12 MAY 2026
Advisory Release Date	12 JUNE 2026
Product	Octopus Server
Operating System	Windows and Linux
Severity	Medium
CVE ID	CVE-2026-8296

Customers who have downloaded and installed any of the 2026.2.13115 versions listed below ("Details") are affected.

Please upgrade your Octopus Server immediately to fix this vulnerability.

Customers who have upgraded Octopus Server to version 2026.2.13115 or higher are not affected.

Octopus Deploy has given this vulnerability a medium rating. This rating was given according to the Octopus Deploy severity levels, which ranks vulnerabilities as critical, high, medium, or low severity.

This is our assessment and you should evaluate its applicability to your own environment.

Details

In affected versions of Octopus Server with certain access levels it was possible to embed a Cross-Site Scripting Payload via artifacts.

The versions of Octopus Server affected by this vulnerability are:

- All 2023.x, 2024.x versions
- All 2025.1.x, 2025.2.x versions, 2025.3.x versions
- All 2025.4.x versions before 2025.4.10678
- All 2026.1.x versions before 2026.1.11451
- All 2026.2.x versions before 2026.2.13114

Fix

To address this vulnerability, we have released Octopus Server version:

- 2025.4.10678
- 2026.1.11451
- 2026.2.13114

The latest versions of Octopus Deploy products can be downloaded from https://octopus.com/downloads and previous versions can be downloaded from https://octopus.com/downloads/previous

Octopus Deploy recommends that you upgrade to the latest version (2026.2.13115). You can download the latest version of Octopus Server from https://octopus.com/downloads

If you can't upgrade to the latest version (2026.2.13115):

If you have feature version...	...then upgrade to this version
2023.x , 2024.x	2025.4.10678 or greater
2025.1.x, 2025.2.x, 2025.3.x	2025.4.10678 or greater
2025.4.x	2025.4.10678 or greater
2026.1.x	2026.1.11451 or greater
2026.2.x	2026.2.13114 or greater

Mitigation

There is no known mitigation for CVE-2026-8296, it is important to upgrade to a fixed version as soon as possible.

Support

If you have any questions or concerns regarding this advisory, please contact our support team https://octopus.com/support.

Exploitation and Public Announcements

Source

This vulnerability was found by asotyc

Recent Security Advisories

- Security Advisory 2026-04
- Security Advisory 2026-03
- Security Advisory 2026-02
- Security Advisory 2026-01
- Security Advisory 2025-07
- Security Advisory 2025-06
- Security Advisory 2025-05
- Security Advisory 2025-04

Products

OCTOPUS SERVER 65 OCTOPUS TENTACLE 4
OCTOPUS DEPLOY TEAMCITY PLUGIN 3 OCTOPUS JAVA SDK 3 HALIBUT 1
KUBERNETES WORKER AND AGENT 1

Tags

SEVERITY/MEDIUM 39 SEVERITY/LOW 25 SEVERITY/HIGH 12
VULNERABILITY/INFORMATION EXPOSURE 7 VULNERABILITY/BROKEN ACCESS CONTROL 6