Security Advisory 2026-01

Aug 20, 2026 · VULNERABILITY/PRIVILEGE ESCALATION SEVERITY/HIGH CVSS/8.7

Summary	Authenticated user can utilize an API endpoint to elevate to Admin permissions
Advisory Number	2026-01
Discovery Date	11 JUN 2026
Patch Release Date	12 JUN 2026
Advisory Release Date	20 AUG 2026
Product	Codefresh
Operating System	Windows and Linux
Severity	High
CVE ID	CVE-2026-12878

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

Please upgrade your Codefresh immediately to fix this vulnerability.

Customers who have upgraded Codefresh to version 2.11.18 or higher are not

Severity

Octopus Deploy has given this vulnerability a high 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 the Codefresh platform an authenticated user can utilize an API endpoint to elevate to Admin permissions

The versions of Codefresh affected by this vulnerability are:

- All 2.x.x versions before 2.11.15

Fix

To address this vulnerability, we have released Codefresh version:

- 2.11.15 that contains a fix for these issues.

The latest versions of the Codefresh product can be downloaded from https://codefresh-io.github.io/cli/installation/download/ and previous versions can be downloaded from https://github.com/codefresh-io/cli/releases

What You Need to Do

If you can't upgrade to the latest version (2.11.18):

If you have feature version...	...then upgrade to this version
2.x.x	2.11.15 or greater

Mitigation

There is no known mitigation for CVE-2026-12878, 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

The Octopus Deploy security team is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during internal testing by Codefresh Platform Team at Octopus Deploy

Products

CODEFRESH 1

Tags

CVSS/8.7 1 SEVERITY/HIGH 1 VULNERABILITY/PRIVILEGE ESCALATION 1

Copyright 2026 CODEFRESH SECURITY ADVISORIES. All Rights Reserved