

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Privilege Escalation Vulnerability in Red Hat OpenShift GitOps
Tracking #:432318146
Date:18-12-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Red Hat OpenShift GitOps that could allow users with limited namespace-level privileges to gain full administrative control over an entire cluster.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability has been identified in Red Hat OpenShift GitOps that could allow users with limited namespace-level privileges to gain full administrative control of an entire cluster. This flaw enables a complete cluster takeover by abusing ArgoCD Custom Resources (CRs).

Vulnerability Details

- **CVE-2025-13888**
- **CVSS Score:** 9.1 **Critical**
- The vulnerability is caused by overly permissive handling of ArgoCD Custom Resources (CRs) by the OpenShift GitOps Operator. A namespace administrator can abuse the sourceNamespaces field in an ArgoCD CR to target privileged namespaces. When processed, the operator automatically creates Roles and RoleBindings in the specified namespace, unintentionally granting elevated permissions. This can allow execution of privileged workloads and potentially lead to full cluster compromise.

Affected Products

- Red Hat OpenShift clusters running vulnerable versions of **OpenShift GitOps** where ArgoCD Custom Resource creation is permitted to non-cluster administrators.

RECOMMENDATIONS:

- Upgrade OpenShift GitOps to the latest patched version.
- Limit administrative privileges to trusted users.
- Audit configurations and permissions.
- Monitor activity for suspicious actions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://nvd.nist.gov/vuln/detail/CVE-2025-13888>