National Cyber Security Centre

2409100130-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical vulnerabilities in Veeam products (CVE-2024-40711, CVE-2024-42024)

Tuesday 10th September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-09-07T17:15:00
Vendor: Veeam
Product: Backup and Replication
CVE ID: CVE-2024-40711
CVSS3.x Score[1]**:** 9.8
EPSS[2]**:** 0.095370000
(For up to date EPSS score: https://api.first.org/data/v1/epss?cve=CVE-2024-40711)

Summary: Veeam have disclosed a critical remote code execution (RCE) vulnerability tracked as CVE-2024-40711, affecting Veeam Backup and Replication. This flaw allows unauthenticated attackers to execute arbitrary code on vulnerable systems. Users are advised to update affected systems to the latest patched version.

Published: 2024-09-07T17:15:00
Vendor: Veeam
Product: Veeam One Agent
CVE ID: CVE-2024-42024
CVSS3.x Score: 9.1
EPSS: 0.095370000
(For up to date EPSS score: https://api.first.org/data/v1/epss?cve=CVE-2024-42024)

Summary: CVE-2024-42024 is a vulnerability that allows an attacker in possession of the Veeam ONE Agent service account credentials to perform remote code execution on the machine where the Veeam ONE Agent is installed.

Products Affected

CVE-2024-40711

- Veeam Backup and Replication versions 12.1.2.172 and all earlier version 12 builds.

CVE-2024-42024

- Veeam ONE versions 12.1.0.3208 and all earlier version 12 builds.

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

Impact

Present in CISA Known Exploited Vulnerability(KEV)[3] catalog: NO
Used by Ransomware Operators: Not Known

CVE-2024-40711
A deserialization of untrusted data vulnerability with a malicious payload can allow an unauthenticated remote code execution (RCE).

CVE-2024-42024
This vulnerability could allow an attacker in possession of the Veeam ONE Agent service account credentials to perform remote code execution on the machine where the Veeam ONE Agent is installed.

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Veeam.

Additional recommendations and mitigations for these vulnerabilities can be found in the respective links below:

- https://www.veeam.com/kb4649
- https://www.veeam.com/products/downloads/latest-version.html

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre