National Cyber Security Centre

2405090138-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in Veeam Service Provider Console

Thursday 9th May, 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

Veeam has released a software update for Veeam Service Provider Console (VSPC) which addresses a critical vulnerability (CVE-2024-29212) which could be exploited to achieve remote code execution. This vulnerability has a CVSS 3.1[1] score of 9.9 and a severity of critical.

Products Affected

- Veeam Service Provider Console versions 4.0 - 8.0 inclusive.

Impact

Exploitation of CVE-2024-29212 could allow an attacker to execute code on the Veeam Service Provider Console (VSPC) host.

To date, there have been no reports of the active exploitation of these vulnerabilities.

Recommendations

The NCSC strongly advises affected organisations to upgrade to a patched version of VSPC.

Further information and some steps that organisations can take can be found here:

- https://www.veeam.com/kb4575
- https://www.veeam.com/kb4441
- https://www.veeam.com/kb4509

[1] https://nvd.nist.gov/vuln-metrics/cvss

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
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie