NCSC

National Cyber Security Centre

2203151328-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerabilities in Veeam Backup & Replication

2022-03-16

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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

Multiple vulnerabilities (CVE-2022-26500, CVE-2022-26501) in Veeam Backup & Replication allow executing malicious code remotely without authentication. The vulnerabilities are:

- CVE-2022-26500
- CVE-2022-26501

The Veeam Distribution Service (TCP 9380 by default) allows unauthenticated users to access internal API functions. A remote attacker may send input to the internal API which may lead to uploading and executing of malicious code. The vulnerabilities have a CVSSv3 score of 9.8.

Products Affected

Veeam Backup & Replication 9.5, 10 & 11

Impact

Potential Remote Code Execution (RCE), data theft, operations disruption, ransomware, denial of service.

Recommendations

The NCSC recommends that affected organisations review the Veeam Advisory and apply the relevant patches as soon as possible.

The following patches are available:

- 11a (build 11.0.1.1261 P20220302)
- 10a (build 10.0.1.4854 P20220304)

Note:

- The patch must be installed on the Veeam Backup & Replication server. Managed servers with Veeam Distribution Service will be updated automatically after installing the patch.
- All new deployments of Veeam Backup & Replication version 11 and 10 installed using the ISO images dated 20220302 or later are not vulnerable.
- If you are using Veeam Backup & Replication 9.5, please upgrade to a supported product version.
- Temporary mitigation of the vulnerabilities: Stop and disable the Veeam Distribution Service. The Veeam Distribution Service is installed on the Veeam Backup & Replication server and servers specified as distribution servers in Protection Groups.

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@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie