National Cyber Security Centre

2405010173-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in NetBackup on Windows (CVE-2024-33672)

Thursday 2nd 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

Published: 2024-04-26
Vendor: Veritas
Product: NetBackup
CVE ID: CVE-2024-33672
CVSS3.0 Score[1]**:** 7.7
EPSS[2]**:** 0.082730000

For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-33672

Summary:

An issue was discovered in Veritas NetBackup before 10.4. The Multi-Threaded Agent used in NetBackup can be leveraged to perform arbitrary file deletion on protected files.

More information related to this issue can be found at the following link(s):
https://www.veritas.com/support/en_US/security/VTS24-001

Products Affected

- Microsoft Windows Operating Systems - Primary Server, Media Server and Clients
- Affected Versions: **10.3.0.1, 10.3, 10.2.0.1, 10.2, 10.1.1, 10.1, 10.0.0.1, 10.0, 9.1.0.1, 9.1, 8.3.0.2.**
- Note: Older unsupported versions may also be affected.

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-427 Uncontrolled Search Path Element

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

Recommendations

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

Additional recommendations and mitigations for CVE-2024-33672 can be found here: https://www.veritas.com/support/en_US/security/VTS24-001

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] 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
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