مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Veritas NetBackup on Windows

Tracking #:432316485

Date:07-11-2024

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a severe privilege escalation vulnerability has been identified in Veritas NetBackup installations running on Windows operating systems.

TECHNICAL DETAILS:

A severe privilege escalation vulnerability has been identified in Veritas NetBackup installations running on Windows operating systems. This vulnerability could allow attackers with write access to the NetBackup installation directory to inject a malicious Dynamic Link Library (DLL) file. Once executed, this could result in the attacker executing arbitrary code within the context of the affected user's security privileges. The vulnerability affects a range of NetBackup versions, including both client and server components.

Vulnerability Details:

- CVE ID: TBD
- Severity: High
- CVSS v3.1 Base Score 7.8

Affected Products:

- Affected Components: NetBackup Client, Primary Server and Media Server Components
- Affected Versions: 10.4.0.1, 10.4, 10.3.0.1, 10.3, 10.2.0.1, 10.2, 10.1.1, 10.1, 10.0.0.1, and 10.0. Older unsupported versions may also be affected.

Fixed Version:

- Upgrade to NetBackup Version 10.5 or
- Upgrade to NetBackup Version 10.4.0.1 and apply hotfix from the Veritas download center.
- Upgrade to NetBackup Version 10.3.0.1 and apply hotfix from the Veritas download center.

Alternate Mitigation (If Immediate Upgrade is Not Possible):

- If upgrading or applying a hotfix is not feasible in the short term, users can mitigate the risk by manually restricting the directory used by NetBackup to load DLLs
  - Create a New Directory: Create a directory named bin under the root drive where NetBackup is installed (e.g., C:\bin if NetBackup is installed on the C: drive). This directory should be empty or contain only trusted executables.
  - Restrict Directory Permissions: Restrict the permissions of this newly created directory to administrative users only. Ensure that non-administrative users cannot write to this directory, preventing attackers from placing malicious DLLs into it.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the alternate Mitigation or upgrade to the fixed version provided by Veritas.

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://www.veritas.com/support/en_US/security/VTS24-012