TLP GREEN

NATIONAL CSIRT-CY

CVE-2026-3991 **05/04/2026**

Symantec DLP Windows Endpoint Vulnerability

Executive Summary

A vulnerability exists in Symantec Data Loss Prevention Agent for Windows. This vulnerability allows an attacker to escalate their privileges to the maximum level.

The issue originated from the compilation of OpenSSL library integration to the Symantec DLP Agent.

This vulnerability carries a CVSS score of 7.8

Attack Path

- The attacker creates the following directory structure at C:\VontuDev\workDir\openssl\output\x64\Release\SSL\.
- He adds a crafted OpenSSL.cnf file and a crafted DLL into this newly created folder.
- He modifies the configuration file of the standard OpenSSL directive dynamic_path to point directly to the attacker's crafted DLL.
- When the Symantec DLP Agent service restarts or triggers an OpenSSL initialization, it reads the malicious configuration file.
- The system loads the attacker's crafted and executes it with SYSTEM privileges.

Solution

Affected users are advised to upgrade to a fixed version below:

- DLP 25.1 MP1
- DLP 16.1 MP2
- DLP 16.0 RU2 HF9
- DLP 16.0 RU1 MP1 HF12
- DLP 16.0 MP2 HF15

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments