

# CVE-2021-27876

## Veritas Backup Exec Agent File Access Vulnerability

CISA KEV since Apr 7, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

An issue was discovered in Veritas Backup Exec before 21.2. The communication between a client and an Agent requires successful authentication, which is typically completed over a secure TLS communication. However, due to a vulnerability in the SHA Authentication scheme, an attacker is able to gain unauthorized access and complete the authentication process. Subsequently, the client can execute data management protocol commands on the authenticated connection.

|                                                                           |                                                      |                                                                  |                                                                                            |
|---------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>75</b>/<sub>100</sub></p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>8.1</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.135</b></p> <p>96.4th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Apr 28, 2023</b></p> <p>KEV since 2023 · listed over a year</p> |
|---------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                            |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.135 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 8.1             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

By using crafted input parameters in one of these commands, an attacker can access an arbitrary file on the system using System privileges.

### Affected and fixed versions

| PACKAGE     | AFFECTED | FIXED IN | SOURCE |
|-------------|----------|----------|--------|
| backup exec | < 21.2   | 21.2     | NVD    |

### Sources

|                        |                                                                                                                                           |                            |                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/advisories/GHSA-9j5v-h34p-h6g6">github.com/advisories/GHSA-9j5v-h34p-h6g6</a>                                 | <b>Additional guidance</b> | <a href="https://veritas.com/content/support/en_US/security/VTS21-001#issue2">veritas.com/content/support/en_US/security/VTS21-001#issue2</a> |
| <b>veritas.com</b>     | <a href="https://veritas.com/support/en_US/security/VTS21-001">veritas.com/support/en_US/security/VTS21-001</a>                           | <b>NVD</b>                 | <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-27876">nvd.nist.gov/vuln/detail/CVE-2021-27876</a>                                         |
| <b>CISA KEV</b>        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                   | <b>ENISA EUVD</b>          | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2021-14614">euvd.enisa.europa.eu/vulnerability/EUVD-2021-14614</a>                   |
| <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2021-27876">evulnable.com/vulnerability-management/cve/CVE-2021-27876</a> |                            |                                                                                                                                               |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.