



# CVE-2005-0773

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2005-0773
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-06-18 04:00:00 UTC
<b>Updated</b>	2011-03-08 02:20:00 UTC
<b>Description</b>	Stack-based buffer overflow in VERITAS Backup Exec Remote Agent 9.0 through 10.0 for Windows, and 9.0.4019 through

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	10.0_rev.5484	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	10.0_rev.5484_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4019	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4170	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4172	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4174	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4202	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4367	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4367_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4454	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4454_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1067.2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1067.3	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1127.1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1151.1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1152	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1152.4	All	All	All

Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1154	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.306	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.307	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1_rev.4691	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1_rev.4691_sp2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	10.0_rev.5484	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	10.0_rev.5484_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4019	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4170	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4172	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4174	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0.4202	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4367	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4367_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4454	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.0_rev.4454_sp1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1067.2	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1067.3	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1127.1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1151.1	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1152	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1152.4	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.1154	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.306	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1.307	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1_rev.4691	All	All	All
Application	<a href="#">Symantec Veritas</a>	<a href="#">Backup Exec</a>	9.1_rev.4691_sp2	All	All	All

## References

### Reference

[Veritas Backup Exec Remote Agent for Windows Servers Authentication Buffer Overflow Vulnerability](#)

[SecurityTracker.com Archives - Veritas Backup Exec Bugs Let Remote Users Execute Arbitrary Code, Crash the System, and Modify the Reg](#)

[Patch summary for Security Advisories VX05-001, VX05-002, VX05-003, VX05-005, VX05-006, VX05-007](#)

[US-CERT Vulnerability Note VU#492105](#)

[VERITAS Software Security Advisory VX05-002](#)

[US-CERT Vulnerability Note VU#492105 - VERITAS Backup Exec Authentication Buffer Overflow Vulnerability](#)

US-CERT Technical Cyber Security Alert 1A05-180A -- VERITAS Backup Exec Software is actively being exploited

Cyber Defense | Accenture

17624

Secunia - Advisories - VERITAS Backup Exec Multiple Vulnerabilities

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**