Security Advisories Relating to Veritas Products

Backup Exec Man-in-The-Middle

May 26, 2011 **SYM11-006**

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
Backup Exec Man-in-The-Middle - Medium			
6.5	10	2.5	AV: A/AC: H/Au: S/C: C/I: C/A: C

Overview

Backup Exec is vulnerable to man-in-the-middle (MiTM) attack due to weakness in communication protocol implementation and lack of validation of identity information exchanged between media server and remote agent.

Affected Products

Product	Version	Build	Solution
Backup Exec for Windows Servers	11.0, 12.0, 12.5	All	Upgrade to Symantec Backup Exec 2010 R3
Backup Exec 2010	13.0, 13.0 R2	All	Upgrade to Symantec Backup Exec 2010 R3

Details

Veritas was notified of a MiTM issue in the manner in which communication protocols are implemented between Backup Exec media server and remote agent. The issue is a result of lack of validation of remote agent identity information exchanged between media server and remote agent. Successful exploitation may result in privilege escalation enabling an attacker to execute post authentication NDMP commands. Successful exploitation requires the attacker to be an authorized user on the network or have unauthorized presence on an authorized system on the network.

Veritas Response

Veritas product engineers verified that the vulnerability exists in the versions of Backup Exec indicated above.

Veritas has released Backup Exec 2010 R3 which establishes trust between Backup Exec remote agent and Backup Exec media server before exchanging any sensitive information. Veritas recommends customers upgrade to this release of Backup Exec which addresses the concern.

Veritas is not aware of any exploitation of, or adverse customer impact from this issue.

Update Information

Customers may obtain Symantec Backup Exec 2010 R3 from their normal support/download locations.

Best Practices

As part of normal best practices, Veritas strongly recommends that customers:

- Restrict access of administration or management systems to privileged users.
- Restrict remote access, if required, to trusted/authorized systems only.
- Run under the principle of least privilege where possible to limit the impact of exploit by threats.
- Keep all operating systems and applications updated with the latest vendor patches.
- Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities

Credit

Veritas dits Nibin Varghese of iViZ Security, for identifying this issue and working with us while we fixed the issue.

References

BID: Security Focus, http://www.securityfocus.com, has assigned Bugtraq ID (BID) 47824 to identify this issue for inclusion in the Security Focus vulnerability database.

CVE: This issue is a candidate for inclusion in the CVE list (http://cve.mitre.org), which standardizes names for security problems. CVE-2011-0546 has been assigned to this issue.

Disclaimer

Veritas Technologies LLC

500 East Middlefield Road

Mountain View, CA 94043

http://www.Veritas.com

Last modified on: April 20, 2016