

(Security Advisory) SYM06-014 Symantec Backup Exec Internal RPC Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-08/msg00257.html>

- *From:* "Secure" <secure@xxxxxxxxxxxxx>
 - *Date:* Fri, 11 Aug 2006 14:19:56 -0700
-

Any further revisions to this information, if required, will be posted to the official advisory located at :
<http://www.symantec.com/avcenter/security/Content/2006.08.11.html>

Symantec Security Advisory

SYM06-014

BID 19479

11 August 2006

Symantec Backup Exec for Windows Server: RPC Interface Heap Overflow, Authorized User Potential Elevation of Privilege

Revision History

None

Severity

Medium

Remote Access Yes Local Access No Authentication Required Yes Exploit publicly available No

Overview

The Backup Exec for Windows Server and Remote Agents for Window Server, also used by the Continuous Protection Server and Backup Exec for Netware

Server, are vulnerable to heap overflows from specifically formatted internal network calls to RPC interfaces.

Supported Product(s Affected

Product Version Build Solution(s) Backup Exec for Windows Server and Remote

Agent 9.1 9.1.4691 HotFix Available Backup Exec for Windows Server and Remote Agent 10.0 10.0.5484 HotFix Available Backup Exec for Windows

(Security Advisory) SYM06–014 Symantec Backup Exec Internal RPC Overflow

Server

and Remote Agent 10.0 10.0.5520 HotFix Available Backup Exec for Windows

Server and Remote Agent 10.1 10.1.5629 HotFix Available Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1

10.1.325.6301 HotFix Available Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1 10.1.326.1401 HotFix Available Backup

Exec Continuous Protection Server Remote Agent for Windows Server 10.1 10.1.326.2501 HotFix Available Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1 10.1.326.3301 HotFix Available Backup

Exec Continuous Protection Server Remote Agent for Windows Server 10.1 10.1.327.401 HotFix Available Backup Exec for Netware Server Remote Agent

for Windows Server 9.1 All HotFix Available Backup Exec for Netware Server

Remote Agent for Windows Server 9.2 All HotFix Available

NOTE: ONLY the products and versions listed above are affected by these issues.

Product versions prior to those listed above are NOT supported.

Customers

running legacy product versions should upgrade and apply available updates.

Details

Tenable Network Security, <http://www.tenablesecurity.com/>, notified Symantec of heap overflow issues they identified in the RPC interfaces of

the Backup Exec for Window Servers and Remote Agents. The Remote Agent for

Windows Server (RAWS) is also used by the Continuous Protection Server as

well as Backup Exec for Netware Server depending on the customer's network environment. The overflows occur due to improper validation and subsequent handling of user input. Successful exploitation would require

the attacker to have authorized but non-privileged access to the network on

which the target system resides. A malicious user who attempted such an attack may cause the targeted application to crash but, if successfully exploited, could potentially execute arbitrary code and gain elevated privilege on the targeted system.

Symantec Response

Symantec engineers did an in-depth review of the reported issues and related file functionality to further enhance the overall security of Symantec Backup Exec for Windows Server and the Remote Agent for Windows Server and to resolve any additional potential concerns. Symantec engineers

have addressed these issues in all currently supported versions of the

(Security Advisory) SYM06–014 Symantec Backup Exec Internal RPC Overflow

products identified above. Security updates are available for all supported products.

Symantec strongly recommends all customers apply the latest security update

as indicated for their supported product versions to protect against threats of this nature.

Symantec knows of no exploitation of or adverse customer impact from these issues.

The patches listed above for affected products are available from the following location:

<http://support.veritas.com/docs/284343> for Symantec Backup Exec for Windows Server and Continuous Protection Server and

<http://support.veritas.com/docs/284623> for Backup Exec for Netware Server.

Best Practices

As part of normal best practices, Symantec recommends:

- * Restrict access to administration or management systems to authorized privileged users

- * Block remote access to all ports not essential for efficient operation

- * Restrict remote access, if required, to trusted/authorized systems only

- * Remove/disable unnecessary accounts or restrict access according to security policy as required

- * Run under the principle of least privilege where possible

- * Keep all operating systems and applications updated with the latest vendor patches

- * Follow a multi-layered approach to security. Run both firewall and antivirus applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats

- * Deploy network 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 latest vulnerabilities

CVE

A CVE Candidate name has been requested from the Common Vulnerabilities and

Exposures (CVE) initiative for this issue. This advisory will be revised accordingly upon receipt of the CVE Candidate name.

This issue is a candidate for inclusion in the CVE list

(<http://cve.mitre.org>), which standardizes names for security problems.

Credit:

Symantec thanks Nicolas Pouvesle from Tenable Network Security for reporting this finding and for excellent coordination while Symantec resolved the issue.