

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

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00052.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Aug 2006 18:34:39 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

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

SUMMARY

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.

DETAILS

Vulnerable Systems:

- * Backup Exec for Windows Server and Remote Agent version 9.1 (9.1.4691)
- * Backup Exec for Windows Server and Remote Agent version 10.0 (10.0.5484)
- * Backup Exec for Windows Server and Remote Agent version 10.0 (10.0.5520)
- * Backup Exec for Windows Server and Remote Agent version 10.1 (10.1.5629)
- * Backup Exec Continuous Protection Server Remote Agent for Windows

Server version 10.1 (10.1.325.6301)

* Backup Exec Continuous Protection Server Remote Agent for Windows

Server version 10.1 (10.1.326.1401)

* Backup Exec Continuous Protection Server Remote Agent for Windows

Server version 10.1 (10.1.326.2501)

* Backup Exec Continuous Protection Server Remote Agent for Windows

Server version 10.1 (10.1.326.3301)

* Backup Exec Continuous Protection Server Remote Agent for Windows

Server version 10.1 (10.1.327.401)

* Backup Exec for Netware Server Remote Agent for Windows Server version 9.1 (All)

* Backup Exec for Netware Server Remote Agent for Windows Server version 9.2 (All)

Tenable Network Security, 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 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>>

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

<<http://support.veritas.com/docs/284623>>

<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

ADDITIONAL INFORMATION

The information has been provided by Nicolas Pouvesle.

The original article can be found at:

<<http://www.symantec.com/avcenter/security/Content/2006.08.11.html>>

<http://www.symantec.com/avcenter/security/Content/2006.08.11.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.