

[NT] CA eTrust AntiVirus WebScan Automatic Update Code Execution (Technical Details)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00034.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Aug 2006 13:30:26 +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>

CA eTrust AntiVirus WebScan Automatic Update Code Execution (Technical Details)

SUMMARY

CA eTrust Antivirus WebScan contains multiple vulnerabilities that can allow remote attackers to gain privileged access or execute arbitrary code. The first vulnerability allows attackers to install arbitrary files. The second vulnerability is due to improper processing of outdated WebScan components. Finally, the third vulnerability is due to improper bounds checking when processing certain user input. Remote attackers can exploit these vulnerabilities to gain escalated privileges or execute arbitrary code.

DETAILS

Vulnerable Systems:

* eTrust AntiVirus WebScan version 1.1.0.1047 and prior

This vulnerability allows remote attackers to execute arbitrary code on systems with affected installations of the Computer Associates eTrust AntiVirus WebScan ActiveX component. Successful exploitation requires that the target user browse to a malicious web page. The vulnerable component

[NT] CA eTrust AntiVirus WebScan Automatic Update Code Execution (Technical Details)

is typically installed as a prerequisite to the free online WebScan found at: <http://www3.ca.com/securityadvisor/virusinfo/scan.aspx>
<http://www3.ca.com/securityadvisor/virusinfo/scan.aspx>

The specific flaw exists during the automatic update process for the WebScan ActiveX component. WebScan allows the initializing web page to specify the location that the component will use to download and install updates through the 'SigUpdatePathFTP' parameter (and potentially the 'SigUpdatePathHTTP' parameter). It downloads the 'filelist.txt' manifest and acquires any update files it lists. There is no verification performed by WebScan to assure the authenticity of the information in the file list or the files themselves. This leads to a possibility of two unique attacks.

In the first attack (CVE-2006-3976), an attacker compresses a malicious file, creates a file listing that includes it and then points the update path to his/her server. The WebScan component will download and decompress the file on the local system. Other components on the system may load the file, and certain files (such as arclib.dll and vete.dll) will be loaded by WebScan itself. If either of these files is replaced by a malicious version, it becomes possible for an attacker to gain control of the system WebScan is installed on during the scanner's initialization process.

In the second attack (CVE-2006-3977), an attacker compresses an outdated version of a legitimate Computer Associates file, and lists an inaccurate timestamp for the file in the update server's file listing. There is no verification on the time/date information provided by the remote server. It is possible for an attacker to install a legitimate but extremely outdated version of virus definition files or engine components to severely limit the scope of the protection provided by WebScan.

Vendor Response:

Computer Associates has addressed this issue in the latest version of their WebScan product. More information from the vendor is available at: <http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=34509>
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=34509>

Disclosure Timeline:

2006.07.17 – Vulnerability reported to vendor
2006.07.26 – Digital Vaccine released to TippingPoint customers
2006.08.07 – Coordinated public release of advisory

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3976>
CVE-2006-3976
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3977>
CVE-2006-3977

ADDITIONAL INFORMATION

[NT] CA eTrust AntiVirus WebScan Automatic Update Code Execution (Technical Details)

The information has been provided by Matthew Murphy, TippingPoint Security Research Team.

The original article can be found at:

<<http://www.tippingpoint.com/security/advisories/TSRT-06-05.html>>

<http://www.tippingpoint.com/security/advisories/TSRT-06-05.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.