

n.runs AG
http://www.nruns.com/
n.runs-SA-2007.024

security(at)nruns.com
25-Jul-2007

Vendor: Computer Associates, <http://www.ca.com>
Affected Products: CA eTrust Antivirus,
<http://www3.ca.com/solutions/product.aspxID=156>
vulnerability : Infinite Loop DoS (remote)
Risk: HIGH

Vendor communication

20070509 Initial notification to CA
20070511 CA Responses
20070511 PGP keys exchange
20070511 PoC files sent to CA
20070515 CA ask for product and version used in the test
20070515 Information requested sent to CA
20070518 CA validates the vulnerabilities
20070724 CA releases the Security Notice to the public
20070725 n.runs AG releases a coordinated disclosure advisory

Overview

Founded in 1976, CA today is a global company with headquarters in the United States and 150 offices in more than 45 countries. They serve more than 99% of Fortune 1000R companies, as well as government entities, educational institutions and thousands of other companies in diverse industries worldwide.

eTrust is an Antivirus developed by Computer Associates. Combined with CA Anti-Spyware for the Enterprise, CA Anti-Virus for the Enterprise provides efficient, centrally-managed, multi-layered protection against a broad range of malware threats.

Description

A remotely exploitable vulnerability has been found in the file parsing engine.

In detail, the following flaw was determined

- Infinite Loop in .CHM files parsing

Impact

This problem can lead to remote engine denial-of-service if an attacker carefully crafts a file that exploits the aforementioned vulnerability. The vulnerability is present in CA eTrust Antivirus software previous to file arclib.dll version 7.3.0.9.

Solution

The vulnerability was reported on 09.May.2007 and an update has been issued to solve this vulnerability through the regular update mechanism.
NOTE Not all products are automatically updated; please refer to the following link to validate
<http://supportconnectw.ca.com/public/antivirus/infodocs/caprodarclib-secnot.asp>

Credit
Bugs found by Sergio Alvarez of n.runs AG.

References
<http://lists.grok.org.uk/pipermail/full-disclosure/2007-July/064895.html>
<http://supportconnectw.ca.com/public/antivirus/infodocs/caprodarclib-secnot.asp>

This Advisory and Upcoming Advisories
http://www.nruns.com/security_advisory.php
<http://www.nruns.com/parsing-engines-advisories.php>

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact securitynruns.com for permission. Use of the advisory constitutes acceptance for use in an as is condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2007 n.runs AG. All rights reserved. Terms of apply.