



CYBSEC S.A.
www.cybsec.com

Advisory Name: Watchfire AppScan QA Remote Code Execution

Vulnerability Class: Buffer Overflow

Release Date: 12/15/2005

Affected Applications:

- AppScan QA 5.0.609 / Subscription 7
- AppScan QA 5.0.134

Affected Platforms:

- Tested on Windows 2000 Server SP4

Local / Remote: Remote

Severity: High

Author: Mariano Nuñez Di Croce

Vendor Status:

- Confirmed, update released.

Reference to Vulnerability Disclosure Policy:

http://www.cybsec.com/vulnerability_policy.pdf

Product Overview:

AppScan QA is an automated web application testing tool that provides QA personnel with security defect analysis and remediation information. Instead of manually searching for security defects, application testers trust AppScan QA to detect security defects and vulnerabilities automatically as an integrated component of enterprise development and testing processes. AppScan QA automates test script creation, modification, and maintenance to ensure reliable and repeatable testing.

Vulnerability Description:

The vulnerability specifically exists in the way AppScan QA processes 401 HTTP responses. If a custom 401 response is specially crafted, containing a WWW-Authenticate header with the Realm field consisting of more than 350 characters, a

buffer overflow occurs, leading to remote code execution with the privileges of the user running AppScan QA.

Proof Of Concept:

A Proof of Concept can be found at <http://www.cybsec.com/vuln/AppScanQA-RemoteCodeExec-PoC.zip>

Mitigating Factors:

For the exploitation to succeed, AppScan QA must be used to analyze a web server specially configured to exploit the vulnerability.

Solutions:

Users should upgrade AppScan QA to Subscription 8, using the AppScan Update Tool.

Vendor Response:

- 10/12/2005: Initial Vendor Contact.
- 10/18/2005: Vendor Confirmed Vulnerability.
- 11/02/2005: Vendor Releases Update.
- 12/15/2005: Advisory Public Disclosure.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at [mnunez {at} cybsec.com](mailto:mnunez@cybsec.com).

For more information regarding CYBSEC: www.cybsec.com