Netquery v4.0 - Security Patch - Modules

NEWS_PDF_AUTHOR: RVirtue

NEWS_PDF_DATE: 2006/11/10 20:40:00

Since announcing the release of Netquery version 4.0, I have been made aware of a potential vulnerability in the output of the client sniffer class that it uses. Details can be seen at SecurityFocus.com.

The issue has been addressed and all current Netquery downloads at VIRtech.org have been updated to correct the problem. For those who have already downloaded, a separate "do-it-yourself" patch kit is available from the same source. A copy of the README.txt file contained in the patch kit is reproduced below.

My sincere apologies to all concerned for the inconvenience.

++++ COPY OF README.TXT FILE IN PATCH PACKAGE ++++

This patch for Netquery version 4.0 addresses a potential vulnerability issue originally reported by Zion Security (http://www.zion-security.com) and subsequently by others, including SecurityFocus (http://www.securityfocus.com) and SecurityTracker (http://www.securitytracker.com).

To install the patch, simply copy both PHP files (nqSniff.class.php and sanitize.inc.php) to the include files subfolder of the Netquery module, overwriting the existing nqSniff.class.php file in that subfolder. There is no need for any updating of Netquery itself. Nor do any of the module and block items in any of Netquery's CMS editions require updating.

Contrary to some of the details contained in the reports cited above, the potential vulnerability affects ALL editions of Netquery as they all use the same adaptation of Roger Raymond's client sniffer class. As output from that class has no built-in sanitizing feature, this patch addresses the issue by including Gavin Zuchlinski's sanitizer functions.

It should be noted that Roger Raymond's client sniffer is a widely used class. It is used, for example, in various functions of several content management systems, including both Postnuke and Xaraya. This patch addresses ONLY those potential vulnerabilities associated with Netquery's uses of its output.

—

Downloads can be found at: VIRtech.org

Since announcing the release of Netquery version 4.0, I have been made aware of a potential vulnerability in the output of the client sniffer class that it uses. Details can be seen at SecurityFocus.com.

The issue has been addressed and all current Netquery downloads at VIRtech.org have been updated to correct the problem. For those who have already downloaded, a separate "do-it-yourself" patch kit is available from the same source. A copy of the README.txt file contained in the patch kit is reproduced below.

My sincere apologies to all concerned for the inconvenience.

++++ COPY OF README.TXT FILE IN PATCH PACKAGE ++++

This patch for Netquery version 4.0 addresses a potential vulnerability issue originally reported by Zion Security (http://www.zion-security.com) and subsequently by others, including SecurityFocus (http://www.securityfocus.com) and SecurityTracker (http://www.securitytracker.com).

To install the patch, simply copy both PHP files (nqSniff.class.php and sanitize.inc.php) to the include files subfolder of the Netquery module, overwriting the existing nqSniff.class.php file in that subfolder. There is no need for any updating of Netquery itself. Nor do any of the module and block items in any of Netquery's CMS editions require updating.

Contrary to some of the details contained in the reports cited above, the potential vulnerability affects ALL editions of Netquery as they all use the same adaptation of Roger Raymond's client sniffer class. As output from that class has no built-in sanitizing feature, this patch addresses the issue by including Gavin Zuchlinski's sanitizer functions.

It should be noted that Roger Raymond's client sniffer is a widely used class. It is used, for example, in various functions of several content management systems, including both Postnuke and Xaraya. This patch addresses ONLY those potential vulnerabilities associated with Netquery's uses of its output.

—

Downloads can be found at: VIRtech.org