netVigilance Inc.
14845 SW Murray Scholls Dr.
Suite 110/311
Beaverton, Oregon 97007
http://www.netvigilance.com
info@netvigilance.com

***** For Immediate Release *****

netVigilance uncovers multiple vulnerabilities in phpMyAdmin network administration console for SQL

Serious threat to corporate databases by XSS attacks discovered, closed.

BEAVERTON, Oregon -- **November 18, 2004** – netVigilance Inc. an authorized distributor of SecureScout., a leading supplier of advanced Network Vulnerability Assessment and Management software for corporations released a security advisory for multiple vulnerabilities discovered in phpMyAdmin; an administration tool for SQL databases over the internet.

The SecureScout security operations center uncovered multiple vulnerabilities in the current stable version of phpMyAdmin that allow attackers to conduct Cross-Site Scripting (XSS) attacks on SQL servers.

XSS attacks almost always focus upon sites which use a session ID stored in a cookie to keep track of a users state, (i.e.: username and password.) The end goal of someone launching a malicious attack such as this; is to steal the cookie of a user of the site, so that they can later impersonate a legitimate user.

This form of attack typically occurs when a user logs in and clicks upon a bogus link, (or moves over it depending on the code), they are redirected to a different site which steals their login credentials.

Cedric Cochin; Director of Product Integration at netVigilance, was quoted as saying “These types of attacks are becoming more and more prevalent. They are used in ‘Phishing’ scams to perpetrate identity theft, unauthorized purchasing, theft of services, etc. All financial institutions, large service providers and ecommerce storefronts are big targets for these types of attacks and should be concerned.” He went on to say “They are also very difficult to trace back to the hacker, since the trail is so cold by the time the attack or theft gets detected.”

SecureScout from netVigilance, works proactively by uncovering network vulnerabilities and providing detailed remediation steps to secure the network before an attack can occur.

Mr. Cochin also stated “The ROI in deploying a state-of-the art vulnerability assessment solution is massive compared to the cost of recovering from a malicious cyber attack. Litigation expenses, damage control, loss of business and customer defection are just some of the costs of not having your network adequately protected.”

The Department of Homeland Security; US-CERT http://www.us-cert.gov/federal/statistics/ - shows that malicious code attacks on corporate networks has increased to 880,167 incidents for the first 6 months of 2004 from 191,306 for the entire year of 2003.

About netVigilance

Founded in 2003, netVigilance delivers best-in-class solutions for protection of corporate networks. With it’s SecureScout™ line of vulnerability assessment tools; netVigilance will ensure increased profitability, increased operational efficiencies, Higher productivity and decreased downtime by increasing the efficiency of network security operations.

The SecureScout™ Security Operations engineers continually uncover vulnerabilities in 3rd party operating systems, equipment, applications and services.

SecureScout™ engineers develop and deploy vulnerability test cases, security alerts, remediation procedures and expert opinion to over 2,000 customers and clients worldwide.

For information contact:

Ron Cox
netVigilance Public Relations
14845 SW Murray Scholls Dr.
Suite 110/310
Beaverton, Oregon 97007
503 997 7838
Ron.cox@netvigilance.com