SecureWorks Security Advisory SWRX-2009-001
McAfee Network Security Manager Cross-Site Scripting (XSS) Vulnerability

Advisory Information

Title: McAfee Network Security Manager Cross-Site Scripting (XSS) Vulnerability
Advisory ID: SWRX-2009-001
Advisory URL: http://www.secureworks.com/ctu/advisories/SWRX-2009-001
Date published: Wednesday, November 11, 2009
CVE: CVE-2009-3565
CVSS v2 Base Score: 4.3 (Medium) (AV:N/AC:M/Au:N/C:N/I:P/A:N)
Date of last update: Wednesday, November 11, 2009
Vendors contacted: McAfee, Inc.
Release mode: Coordinated release
Discovered by: Daniel King, SecureWorks

Summary

McAfee Network Security Manager is vulnerable to cross-site scripting (XSS) caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using vulnerable parameters in a specially-crafted URL to execute script in a victim's web browser within the security context of the Network Security Manager site.

Affected Products

McAfee Network Security Manager (NSM), version 5.1.7.7 (default configuration).

It is unknown which other versions, if any, are affected as of November 11, 2009.

Vendor Information, Solutions and Workarounds

McAfee has provided a new release to address this security flaw. Upgrade NSM software to NSM 5.1.11.6 or above, available for McAfee NSM clients at:

https://secure.nai.com/apps/downloads/my_products/login.asp

More information is available from McAfee at:

McAfee Security Bulletin SB10004
Intrushield NSM update fixes XSS flaw
https://kc.mcafee.com/corporate/index?page=content&id=SB10004

Follow best practices of placing the security management console on a segregated management network. Apply restrictive, default-deny firewall policies to protect these assets from access by unauthorized users.

Do not perform administrative access of security management consoles from computers exposed to the Internet through web browsing, email, and other applications. Lock down and heavily monitor systems used to perform administrative tasks such as accessing security management consoles.

Details

User-controllable input supplied by the “iaction” and “node” parameters to the “Login.jsp” page is not properly sanitized for invalid or malicious content prior to being returned to the user in dynamically generated web content. This condition may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

SecureWorks Risk Scoring

Likelihood: 2 – Best practice is to deploy the management console web application on a segmented management network.

Impact: 5 – Control over security appliances managed by the management console.

CVSS Severity (version 2.0)

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized modification
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Impact Subscore: 2.9
Exploitability Subscore: 8.6
CVSS v2 Base Score: 4.3 (Medium) (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Proof of Concept

The following example URLs demonstrate user-controllable JavaScript being executed in the context of the McAfee Network Security Manager website.

https://x.x.x.x/intruvert/jsp/module/Login.jsp?password=&Login%2bID=&node=&iaction=precreatefcb14"><script>alert('XSS')</script>8b3283a1e57

https://x.x.x.x/intruvert/jsp/module/Login.jsp?password=&Login%2bID=&node=8502a"><script>alert(1)</script>2aa99b60533&iaction=precreatefcb14"><script>alert(‘XSS’)</script>8b3283a1e57

Revision History

1.0 November 11, 2009 – Initial advisory release

PGP Keys

This advisory has been signed with the PGP key of the SecureWorks Counter Threat Unit(SM), which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About the SecureWorks Counter Threat Unit℠

Our expert team of threat researchers, also known as the SecureWorks Counter Threat Unit℠, identifies and analyzes emerging threats and develops countermeasures, correlations and SOC processes to protect clients' critical information assets. The CTU frequently serves as an expert resource for the media, publishes technical analyses for the security community and speaks about emerging threats at security conferences. Leveraging our security technologies and a network of industry contacts, the CTU tracks leading hackers and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables the CTU to identify threats as they emerge and develop countermeasures that protect our clients before damage occurs.

About SecureWorks

With over 2000 clients, SecureWorks has become one of the leading Security as a Service providers safeguarding more organizations 24x7 than any other vendor. SecureWorks focuses exclusively on information security services and was recently positioned in the Leader's Quadrant in Gartner's Magic Quadrant for Managed Security Services Providers (MSSPs). SecureWorks Security Information and Event Management (SIEM) platform augmented with applied security research and 100% GIAC-certified experts protects clients with our award-winning Managed Security Services and SIM On-Demand solution.

Disclaimer

This advisory may not be edited or modified in any way without the express written consent of SecureWorks, Inc. If you wish to reprint this advisory or any portion or element thereof, please contact

The information within this advisory may change without notice. The most recent version of this advisory may be found on the SecureWorks web site at www.secureworks.com for a limited period of time. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or spread of this information.