Security Advisory SWRX-2013-001

Cisco NAC Appliance (Cisco Clean Access / Perfigo) authentication cross-site scripting (XSS)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Cisco NAC Appliance (Cisco Clean Access / Perfigo) authentication cross-site scripting (XSS)
Advisory ID: SWRX-2013-001
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2013-001/
Date published: Wednesday, January 30, 2013
CVE: CVE-2012-6029
CVSS v2 base score: 4.3
Date of last update: Wednesday, January 30, 2013
Vendors contacted: Cisco Systems, Inc.
Release mode: Coordinated
Discovered by: Craig Lambert, Dell SecureWorks

Summary

The Cisco NAC Appliance (formerly, Cisco Clean Access) "enforces security policy compliance on all devices that attempt to gain access" to organizations' infrastructure. A common application of Cisco NAC is to "provide easy and secure guest access."

A vulnerability exists in the web-based authentication functions of Cisco NAC Appliance versions up to and including 4.9.2. The vulnerability involves insufficient input validation of URL parameters. Successful exploitation may allow an attacker to retrieve session cookies, steal recently submitted data, or launch additional attacks.

Affected products

This vulnerability affects supported versions of the Cisco NAC Appliance up to and including 4.9.2.

Vendor information, solutions and workarounds

Cisco has released information in
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2012-6029

The vulnerability will be addressed in versions 4.8.4 and 4.9.3.

Details

A vulnerability exists in Cisco NAC Appliance (Cisco Clean Access) versions up to and including 4.9.2 due to insufficient input validation affecting the web authentication functions "`perfigo_weblogin.jsp`" and "`perfigo_cm_validate.jsp`". User-controllable input supplied to `perfigo_weblogin.jsp` ("`cm`" or "`uri`" parameters) and `perfigo_cm_validate.jsp` ("`cm`", "`provider`", "`session`", "`uri`", "`userip`" or "`username`" parameters) is not properly sanitized for illegal or malicious data prior to being returned to the user in dynamically generated web content. Remote attackers could leverage this issue to conduct reflected cross-site scripting (XSS) attacks via specially crafted requests. When loaded, arbitrary script or HTML

code injected into the affected parameter is executed in a target user's browser session in the security context of a vulnerable website. Successful exploitation may allow an attacker to retrieve session cookies, steal recently submitted data, or launch additional attacks.

CVSS severity (version 2.0)

Access Vector: Network
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 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Proof of concept

Request URL ("uri" parameter):

```
hxxps://ciscocleanaccess.target/auth/perfigo_weblogin.jsp?cm=ws32vklm&uri=http%3A%2F%2
Fdell.com%2Ff50a2"><script>alert(document.cookie)</script>feffec9bba
```

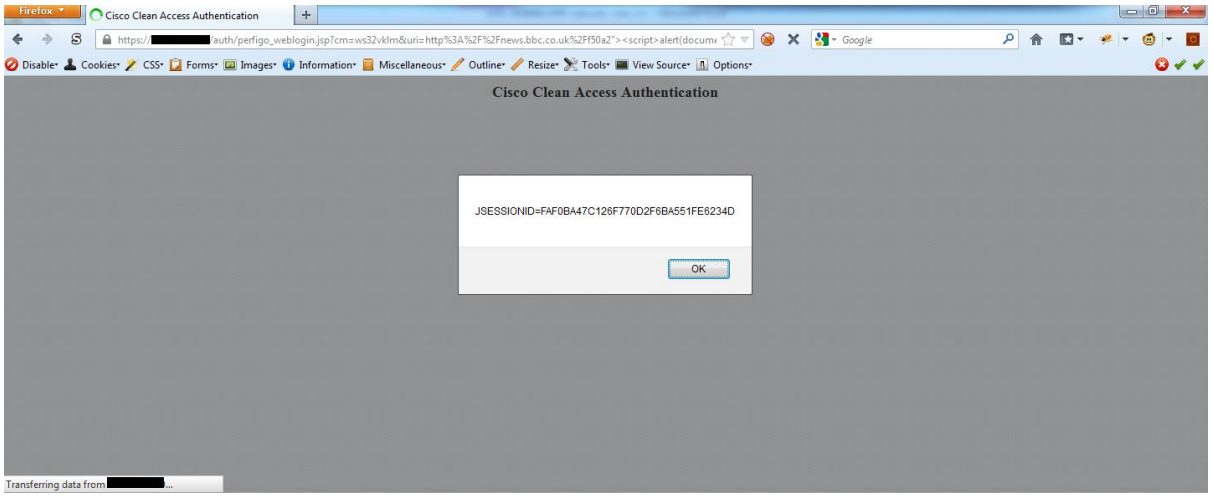

Figure 1. Screenshot of proof-of-concept cookie in XSS pop-up. (Source: Dell SecureWorks)

```
    -->
  </script>
</head>

<body onLoad="javascript:load();">

  <div align="center" class="title">

    Guest Access Authentication
  </div>

  <form method="post" name="loginform" action="../auth/perfigo_cm_validate.jsp" target="_parent">
          <div align="center">
              <input type="hidden" name="reqFrom" value="perfigo_tiny_login.jsp"/>
              <input type="hidden" name="uri" value="http://news.bbc.co.uk/"/>
              <input type="hidden" name="cm" value="ws32vklmdd8ac"><script>alert(1)</script>5e517455617"/>
              <input type="hidden" name="userip" value="192.168.66.74"/>
              <input type="hidden" name="session" value=""/>
              <input type="hidden" name="pm"/>
              <input type="hidden" name="index" value="0"/>
              <input type="hidden" name="pageid" value="-1"/>
              <input type="hidden" name="compact" value="true"/>


                  <input type="hidden" name="registerGuest" value="NO"/>
              <input type="hidden" name="userNameLabel" value="Email address"/>
              <input type="hidden" name="passwordLabel" value="Password"/>
              <input type="hidden" name="guestUserNameLabel" value="Guest ID"/>
              <input type="hidden" name="guestPasswordLabel" value="Password"/>
```

Figure 2. Screenshot of proof-of-concept injected JavaScript. (Source: Dell SecureWorks)

Revision history

1.0 2013-01-30: Initial advisory release

PGP keys

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

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer