Security Advisory SWRX-2012-001

Cisco IronPort Encryption Appliance administrative interface DOM-based cross-site scripting vulnerability

Dell SecureWorks Counter Threat Unit Intelligence Services

Advisory Information

Title: Cisco IronPort Encryption Appliance administrative interface DOM-based cross-site scripting vulnerability
Advisory ID: SWRX-2012-001
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2012-001/
Date published: Monday, February 13, 2012
CVE: CVE-2012-0340
CVSS v2 base score: 4.3
Date of last update: Monday, February 13, 2012
Vendors contacted: Cisco Systems, Inc.
Release mode: Coordinated
Discovered by: Craig Lambert, Dell SecureWorks

Summary

A vulnerability exists in Cisco IronPort Encryption Appliance due to improper input validation of user-controlled input to the web-based administrative interface. User-controlled input supplied to the login page via the URL parameters/values is not properly sanitized for illegal or malicious content prior to being returned to the user in dynamically generated web content. A remote, unauthenticated attacker could exploit this vulnerability to perform DOM-based cross-site scripting (XSS) attacks, potentially resulting in the compromise of administrator sessions on the Cisco IronPort Encryption Appliance device.

Affected products

Cisco IronPort Encryption Appliance prior to version 6.5.3.

Vendor information, solutions and workarounds

Cisco's IntelliShield alert can be found at
http://tools.cisco.com/security/center/viewAlert.x?alertId=25045

Users of Cisco IronPort Encryption Appliance should upgrade to the latest version (currently 6.5.5).

Details

Cisco IronPort Encryption Appliance is an email encryption gateway, providing secure email delivery services. From the vendor's description: "The Cisco IronPort Encryption Appliance is the most comprehensive email encryption gateway available today. Whether you're looking to meet compliance requirements, improve customer and partner trust, or protect intellectual property, the Cisco IronPort Encryption Appliance provides the flexibility and scalability to support all secure messaging requirements on a single platform—making it the ideal email solution for data loss prevention."

Older versions of the Cisco IronPort Encryption Appliance web-based administrative interface are vulnerable to DOM-based cross-site scripting.

A remote, unauthenticated attacker could target Cisco IronPort Encryption Appliance administrative users with crafted URLs containing malicious JavaScript, potentially compromising Cisco IronPort Encryption Appliance administrator sessions and affecting the confidentiality, integrity and availability of the appliance.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Medium
Authentication: None
Impact type: Allows unauthorized modification
Confidentiality impact: None
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 4.3
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 8.6
CVSS v2 vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Proof of concept

The `/admin/` JavaScript constructs three frames from the `document.location` that are used to populate a `<frameset>` further down the page. `document.location` can be influenced as follows, resulting in JavaScript executing in the user's browser:

https://192.168.1.1/admin/?header=%22%20onload=%22alert%281%29%22//&body=body&footer=footer

The supplied string is: `?header=%22%20onload=%22alert%281%29%22//&body=body&footer=footer`

The vulnerable JavaScript is highlighted below:

```
var passed;
passed = location.search ?
    unesc(location.search.substring(1)) + '&' :
    '';
var myHeader = passed ?
    passed.substring(0, passed.indexOf('&')) :
    'PostXShell.action';

passed = passed.substring(passed.indexOf('&') + 1);

var myBody = passed ?
    passed.substring(0, passed.indexOf('&')) :
    'home.action';

passed = passed.substring(passed.indexOf('&') + 1);

var myFooter = passed ?
    passed.substring(0,passed.indexOf('&')) :
    '';
```

```
if (top != self)
{
    if (document.images)
        top.location.replace(self.location.href);
    else
        top.location.href = self.location.href;
}
else
{
    if (document.images)
    {
        pxi87143548 = new Image();

        document.write('<frameset framespacing=0 border=false ' +
            'frameborder=0 rows="' + topRows + ',*' +
            (myFooter ? ',50' : '') + '">');
        document.write(' <frame name=header scrolling=auto ' +
            'marginwidth=0 marginheight=0 noresize src="' + myHeader +
'">');
        document.write(' <frame name=body scrolling=auto ' +
            'marginwidth=5 marginheight=5 noresize src="' + myBody + '">');
        if (myFooter)
            document.write(' <frame name=footer scrolling=no ' +
                'marginwidth=0 marginheight=0 noresize src="'+ myFooter +
                '">');
        document.write('<\/frameset>');
    }
    else
    {

        document.write('<frameset framespacing=0 border=false ' +
            'frameborder=0 rows="' + topRows + ',*">');
        document.write(' <frameset rows="100%,*">');
        document.write(' <frame name=header scrolling=auto ' +
            'marginwidth=0 marginheight=0 noresize src="' + myHeader +
'">');
        document.write(' <frame name=pxi87143548 scrolling=no ' +
            'marginwidth=0 marginheight=0 noresize src="blank.htm">');
        document.write(' <\/frameset>');
        document.write(' <frameset rows="*' + (myFooter ? ',50' : '') +
'">');
        document.write(' <frame name=body scrolling=no ' +
            'marginwidth=5 marginheight=5 noresize src="' + myBody + '">');
        if (myFoooter)
            document.write(' <frame name=footer scrolling=no ' +
                'marginwidth=0 marginheight=0 noresize src="'+ myFooter +
                '">');
        document.write(' <\/frameset>');
        document.write('<\/frameset>');
    }
}
//-->
```

```
</script></head><frameset framespacing="0" border="false" frameborder="0"
rows="100,*,50"> <frame name="header" marginwidth="0" marginheight="0"
noresize="noresize" src="header=" onload="alert(1)" scrolling="auto"> <frame
name="body" marginwidth="5" marginheight="5" noresize="noresize" src="body=body"
scrolling="auto"> <frame name="footer" marginwidth="0" marginheight="0"
noresize="noresize" src="footer=footer" scrolling="no"></frameset>
<noscript>
```

Figure 1. User-supplied JavaScript inserted into the constructed frameset.

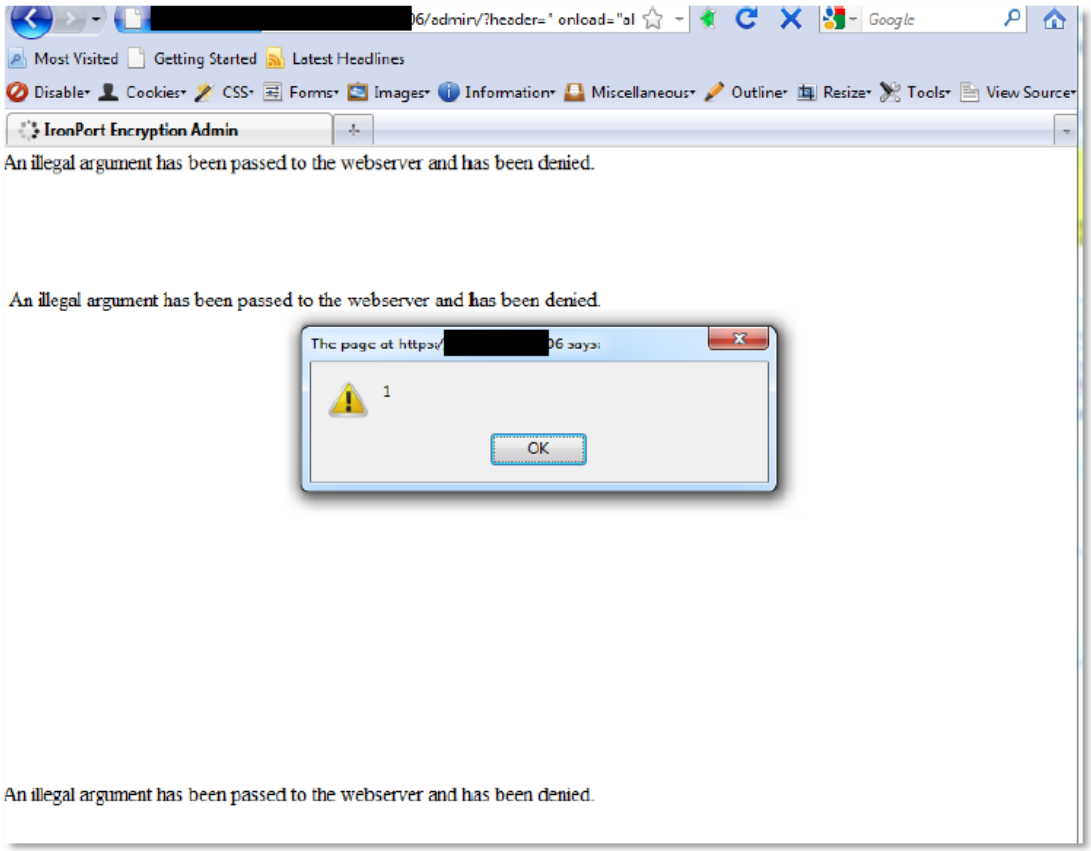

Figure 2. JavaScript "alert" proof of concept.

Revision history

1.0 2012-02-13: 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