



# Security Advisory SWRX-2012-007

## F5 BIG-IP® Configuration Utility persistent cross-site scripting vulnerability

---

### Dell SecureWorks Counter Threat Unit™ Threat Intelligence

#### Advisory Information

**Title:** F5 BIG-IP® Configuration Utility persistent cross-site scripting vulnerability

**Advisory ID:** SWRX-2012-007

**Advisory URL:** <http://www.secureworks.com/research/advisories/SWRX-2012-007/>

**Date published:** Tuesday, October 2, 2012

**CVE:** CVE-2012-2975

**CVSS v2 base score:** 4.3

**Date of last update:** Tuesday, October 2, 2012

**Vendors contacted:** F5

**Release mode:** Coordinated

**Discovered by:** Roger Wemyss, Dell SecureWorks

#### Summary

A vulnerability exists in the BIG-IP® Configuration Utility due to improper sanitization of the "Top Requested URLs" table on the Overview: Traffic page. Malicious content is not properly sanitized before being stored and is later returned to an administrator in dynamically generated web content. Remote attackers could leverage this vulnerability to conduct persistent cross-site scripting attacks. When a user navigates to the Overview: Traffic page within the BIG-IP Configuration Utility, the content of the "Top Requested URLs" table is loaded into the affected JavaScript array and is executed in the user's browser session. Successful exploitation may aid an attacker in retrieving session cookies, stealing recently submitted data, or launching further attacks.

#### Affected products

F5 BIG-IP Application Security Manager 11.2.0 hotfix 1:

<http://www.f5.com/products/big-ip/application-security-manager.html>

#### Vendor information, solutions and workarounds

The vendor has released a security advisory that addresses this vulnerability. F5's Bug ID for the issue is SOL13838. For more information, please refer to F5's notification at:

<http://support.f5.com/kb/en-us/solutions/public/13000/800/sol13838.html>

#### Details

The BIG-IP Configuration Utility is a web management console for F5 devices. There is a persistent cross-site scripting vulnerability in the "Top Requested URLs" table on the "Overview: Traffic" page within this interface. The system stores the top requested URL information but improperly sanitizes the "URL" field when it is displayed within the "Top Requested URLs" Table in the GUI.

## Security Advisory SWRX-2012-007 F5 BIG-IP® Configuration Utility persistent cross-site scripting vulnerability

---

In the BIG-IP Configuration Utility, the Overview: Traffic page is accessed by selecting the "Application Security", "Overview", "Traffic" option under the "Main" tab. When a user navigates to the "Overview: Traffic" page within the BIG-IP Configuration Utility, the content of the "URL" field in the "Top Requested URLs" table is loaded into the affected JavaScript array and is executed in the user's browser session.

Successful exploitation of this vulnerability could lead to full remote administrative access of the vulnerable products. After obtaining administrative access, an attacker may be able to create, modify, or delete user accounts, read stored messages, purge system logs, and access sensitive and confidential information.

### CVSS severity (version 2.0)

**Access vector:** Network exploitable  
**Access complexity:** Medium  
**Authentication:** Not required to exploit  
**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

Entering the following content in the URL of a protected web server will generate events that reproduce the issue:

```
http://<protected server IP>/<script>alert('exampletext')</script>
```

This vulnerability relies on the URL being requested enough times to be displayed in the "Top Requested URLs" table on the traffic overview page.

---

### Revision history

1.0      2012-10-02: 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

Copyright © 2012 Dell SecureWorks

This advisory may not be edited or modified in any way without the express written consent of Dell SecureWorks. Permission is hereby granted to link to this advisory via the Dell SecureWorks website or use in accordance with the fair use doctrine of U.S. copyright laws. See the Dell SecureWorks terms of use at [http://www.secureworks.com/contact/terms\\_of\\_use/](http://www.secureworks.com/contact/terms_of_use/) for additional information.

The most recent version of this advisory may be found on the Dell SecureWorks website at [www.secureworks.com](http://www.secureworks.com). The contents of this advisory may change or be removed from the website without notice. 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 Dell SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or further publication or disclosure of this information.