Security Advisory SWRX-2012-002

Imperva SecureSphere persistent cross-site scripting vulnerability

Dell SecureWorks Counter Threat Unit Intelligence Services

Advisory Information

Title: Imperva SecureSphere persistent cross-site scripting vulnerability
Advisory ID: SWRX-2012-002
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2012-002/
Date published: Tuesday, February 14, 2012
CVE: CVE-2011-4887
CVSS v2 base score: 4.3
Date of last update: Tuesday, February 14, 2012
Vendors contacted: Imperva
Release mode: Coordinated
Discovered by: Roger Wemyss, Dell SecureWorks

Summary

A vulnerability exists in Imperva SecureSphere due to improper sanitization of the "username" field in the Violations Table. 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 Violations page within the SecureSphere administrative GUI, the content of the "username" field 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

Imperva SecureSphere Web Application Firewall 9.0:

http://www.imperva.com/products/wsc_web-application-firewall.html

Vendor information, solutions and workarounds

The vendor has released SecureSphere 9.0 patch 1 that addresses this vulnerability. Imperva's Bug ID for the issue is 37929. For more information, please refer to Imperva's notification at http://www.imperva.com/resources/adc/adc_advisories_response_secureworks_CVE-2011-4887.html.

Details

The Imperva SecureSphere GUI is a centralized management console for Imperva WAF devices. There is a persistent cross-site scripting vulnerability in the Violations section of this interface. SecureSphere properly detects the cross-site scripting payload destined for the protected server as being malicious and records an event. The system's event database stores this information but improperly sanitizes the "username" field when it is displayed within the Violations Table in the GUI. This condition allows JavaScript events to be processed when violations are added to the "items" array.

In the SecureSphere GUI, the Violations page is accessed by selecting the Violations option of the Monitor tab. When a user navigates to the Violations page within the SecureSphere administrative GUI, the content of the "username" field in the Violations 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 "username" field of a protected web server will generate events that reproduce the issue:

```
<script>alert('exampletext')</script>
```

This vulnerability relies on SecureSphere recognizing the input as being a username and populating it accordingly within the Violations Table.

Revision history

1.0 2012-02-14: 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