CSS10-01: Imperva SecureSphere Web Application Firewall and Database Firewall Bypass Vulnerability

April 5, 2010

BACKGROUND

The Imperva™ SecureSphere® Web Application Firewall protects web applications and sensitive data against sophisticated attacks and brute force attacks, stops online identity theft, and prevents data leaks from applications. The Imperva™ SecureSphere® Database Firewall monitors and proactively protects databases from internal abuse, database attacks, and unauthorized activity. *(Source: http://www.imperva.com/products/securesphere-data-security-suite.html)*

SUMMARY

Imperva SecureSphere Web Application Firewall and Database Firewall products can be bypassed by appending specially crafted data to requests. Protection provided by the Imperva device against attacks such as SQL injection and Cross-Site Scripting is negated, allowing unfiltered requests through to protected applications.

SEVERITY RATING

Rating: High Risk - CVSS 7.8 (AV:N/AC:L/Au:N/C:N/I:C/A:N)
Impact: Bypass security control
Where: Remote

THREAT EVALUATION

An attacker can use this flaw to bypass firewall protections. Anyone with the ability to interact with protected web applications and databases can exploit this vulnerability. Only minimal skill is required and the bypass can be incorporated into existing exploitation frameworks and security testing tools. Exploitation of this issue does not permanently affect the device; each evasion request must contain the bypass payload.

IDENTIFYING VULNERABLE INSTALLATIONS

Administrators can identify the current version in use by going to the Licensing menu in the administration console. Versions less than those identified in the Solutions section below are vulnerable.

DETECTING EXPLOITATION

The Imperva device provides no indication when this vulnerability is exploited. If other controls are in place such as network traffic monitors, IDS/IPS, or web filters, these should be configured to alert on payloads containing attack patterns.

AFFECTED SOFTWARE

This vulnerability affects SecureSphere G-series and Database Firewalls running versions the Web Application and Database Firewall product prior to March 9, 2010. This includes all versions of SecureSphere from 5.0 through 7.0.

SOLUTION

The vendor has released patches for affected versions to address this issue. Customers are strongly encouraged to apply the update as soon as possible. Refer to http://www.imperva.com/resources/adc/adc_advisories_response_clearskies.html for upgrade instructions. No reliable workaround is available.

The vendor has provided the following version and patch data:

Version	Patch Number
7.0.0.7078	Patch 11
7.0.0.7061	Patch 11
6.2.0.6463	Patch 24
6.2.0.6442	Patch 24
6.0.6.6302	Patch 30
6.0.6.6274	Patch 30
6.0.5.6238	Patch 30
6.0.5.6230	Patch 30
6.0.4.6128	Patch 30
5.0.0.5082	Patch 30
6.0.4.6128 on XOS 8.0/5	ssgw-6128-CBI10
7.0.0.7078 on XOS 8.5.3	ssgw-7.0.0.7267-CBI28

VULNERABILITY ID

CVE-2010-1329

TIME TABLE

2009-08-31 – Vendor notified.
2010-03-09 – Vendor released patched firmware.
2010-04-05 – Public notification

CREDITS

Scott Miles and Greag Johnson, Clear Skies Security, identified this flaw.

Clear Skies would like to thank Mike Sanders and Accuvant Labs for their assistance in clarifying and working with the vendor to correct this issue.

LEGAL NOTICES

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing and is subject to change without notice. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. The author is not liable for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.