CSS12-11: Verifone VeriCentre Web Console SQL Injection Vulnerability

November 02, 2012

BACKGROUND

VeriCentre is the next-generation estate management system that significantly reduces costs, improves customer service, and provides new revenue opportunities. It delivers unprecedented productivity and flexibility with an array of capabilities and automation for any size installed base or multi-application environment. And since it works with all Vx Solutions payment devices, VeriCentre can be deployed across all vertical markets around the globe. *(Source: http://www.verifone.com/estate-management/vericentre.aspx)*

SUMMARY

A function in the VeriCentre web application is vulnerable to SQL Injection. Input to the affected function can be provided that manipulates the SQL query issued to the application database. By constructing the appropriate input, the attacker can issue any commands against the database.

SEVERITY RATING

Rating: High Risk - CVSS 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)
Impact: Bypass web application control
Where: Remote

THREAT EVALUATION

This issue is in a publicly accessible function on the web site that could be exploited by any individual (or automated worm) via the intranet, although the vulnerable functions are not directly referenced from the main web page. Authentication is required in order to identify this vulnerability. The presence of telltale error messages greatly increases the likelihood that this issue would be identified and exploited.

IDENTIFYING VULNERABLE INSTALLATIONS

Administrators can identify the vulnerability by issuing the following request to the web application. The TerminalId, ModelName, and ApplicationName parameters are all susceptible to injection.

http://1.2.3.4/WebConsole/terminal/paramedit.aspx?TerminalId=%27%2bconvert%28int,@@version%29%2b%27&ModelName=xxxx&ApplicationName=xxxx&ClusterId=

DETECTING EXPLOITATION

The VeriCentre web application provides no indication when this vulnerability is exploited other than possibly the web logs. 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 all VeriCentre Web Consoles prior to version 2.2 build 36.

SOLUTION

The vendor has released updated code and all customers are encouraged to update as soon as possible to Web Console 2.2 build 36 or higher.

VULNERABILITY ID

CVE-2012-4951

TIME TABLE

2012-04-05 – Vulnerability identified.
2012-09-14 – CERT notified.
2012-11-01 – Vendor released security patch at approximately this date.

CREDITS

Cory Eubanks, Clear Skies Security, identified this flaw.

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.