CSS11-01: Proofpoint Protection Server Multiple Vulnerabilities

May 2, 2011

BACKGROUND

The Proofpoint Enterprise Protection™ protects mission-critical email infrastructure from outside threats including spam, phishing, unpredictable email volumes, malware and other forms of objectionable or dangerous content before they hit the enterprise perimeter. *(Source: http://www.proofpoint.com/products/enterprise-protection-email-security.php)*

SUMMARY

The Proofpoint Protection Server contains multiple vulnerabilities including authentication bypass, command injection, SQL injection, directory traversal, and insufficient authorization checks for authenticated pages.

Clear Skies Security conducted the testing of the Proofpoint appliance in the course of performing a standard Penetration Test for a customer. Thorough testing of the Proofpoint appliance was not the goal of this project; as such, this advisory is not intended to encapsulate all vulnerabilities associated with the appliance, and it is possible that additional instances of the discovered vulnerabilities may be present in other areas of the appliance interface.

SEVERITY RATING

Rating:	High Risk - CVSS 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Impact:	Multiple Vulnerabilities
Where:	Remote

TECHNICAL DETAILS

ENDUSER AUTHENTICATION BYPASS

User-level access to the Proofpoint mail filter web interface can be obtained as any available user without providing the user's login credentials.

PATH TRAVERSAL ALLOWS ACCESS TO SYSTEM FILES

Arbitrary files on the Proofpoint appliance can be obtained by manipulating a flaw in the web interface.

PROOFPOINT SQL INJECTION

A publicly accessible function in the Proofpoint interface is vulnerable to SQL Injection.

PROOFPOINT COMMAND INJECTION

A function in the Proofpoint web interface can be manipulated into executing any command on the server.

PROOFPOINT FORCED BROWSING / INSUFFICIENT PAGE AUTHORIZATION

Some administrative modules are accessible without authenticating with the application.

THREAT EVALUATION

An attacker can use these flaws to compromise the Proofpoint Protection Server, and gain access to application data, configuration files, log files, and shell access. Anyone with the ability to manipulate web application calls can exploit these vulnerabilities. Only minimal skill is required for all the vulnerabilities except the authentication bypass. All of these findings can easily be incorporated into existing exploitation frameworks and security testing tools.

IDENTIFYING VULNERABLE INSTALLATIONS

Administrators can identify the current version in use by going to the administration console and viewing the version displayed on the login page. Versions equal to and less than those identified in the Solutions section below are vulnerable.

DETECTING EXPLOITATION

The web server log files may provide an 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 and block on payloads containing path traversals, SQL and command injection attack patterns.

AFFECTED SOFTWARE

These vulnerabilities have been confirmed to affect the Proofpoint Protection Server. The version displayed on the web application login page, port 10000, displays 6.0. However, once shell access was obtained the following version was observed.

```
Proofpoint Messaging Security Gateway 6.2.0.263:6.2.0.237
```

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 https://support.proofpoint.com/article.cgi?article_id=338413 for instructions. (CTS username and password required) for upgrade instructions.

RECOMMENDED WORKAROUND

Restrict access to the Proofpoint web application, especially the admin functionality either with network ACLs and/or an additional layer of authentication such as VPN. If an Intrusion

Prevention System or Web Application Firewall is in place, it may be possible to configure blocking rules that match SQL statements, relative directory paths ("../") and null bytes (%00). Consider rejecting any string containing characters outside the pattern [a-zA-Z1-9\.-\@].

The vendor has provided the following version and patch data:

Version	Patch Number
5.5.3, 5.5.4 and 5.5.5	Patch 1044
6.0.2	Patch 1045
6.1.1 and 6.2.0	Patch 1046

VULNERABILITY ID

United States Computer Emergency Readiness Team - VU#790980
http://www.kb.cert.org/vuls/id/790980

TIME TABLE

2011-02-02 – Vendor notified.
2011-02-22 - Vendor released patched software
2011-05-02 - Public notification

CREDITS

Scott Miles, Clear Skies Security, identified these flaws.

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.