security-assessment.com

# Vulnerability Advisory

| | |
|---|---|
| **Name** | Symantec Web Gateway Multiple Vulnerabilities |
| **Vendor Website** | https://www.symantec.com/ |
| **Affected Software** | Symantec Web Gateway <= 5.2.2.118 |
| **Date Released** | 17th September 2015 |
| **CVE Numbers** | CVE-2015-6547, CVE-2015-6548 |
| **Researchers** | Daniel Jensen |

## Description

Symantec Web Gateway contains multiple instances of SQL injection and command injection, allowing an authenticated attacker to read information from the database, and execute operating system commands as root.

## Exploitation

**SQL Injection**

A time based blind SQL Injection is present in the "edit_alert.php" page, in the alertid and applianceid parameters. This is due to insecure construction of SQL commands. Although the mysql_real_escape_string function is used, this does not fully sanitise strings in the case of insecure construction. The alertid and applianceid variables are passed to the mysql_real_escape_string without being quoted, and an attacker may insert additional SQL after the variable, as shown below.

The following screenshots show the vulnerable code in edit_alert.php, and an example request to show the SQL injection.

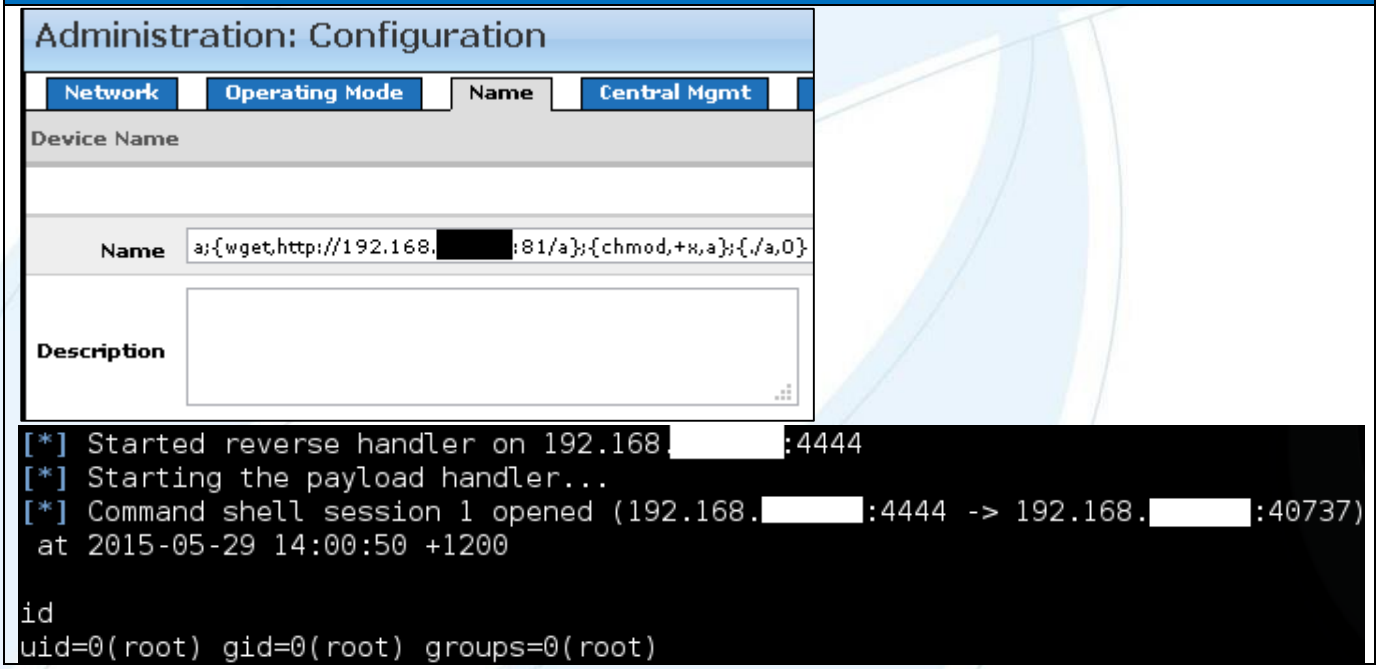
**Proof of Concept**

```
490:    $query = "select * from mi5_alert where alertid = $alertid AND applianceid = $applianceid";
491-
492-   $query_escape = mysql_real_escape_string($query);
493-   //trigger_error("query_escape #1 $query_escape");  //vul test ok - paul
494-   $result = @mysql_query($query_escape);
495-
```

```
GET /spywall/edit_alert.php?alertid=2%20AND%20(SELECT%20*%20FROM%20(SELECT%20(SLEEP(10)))A)&applianceid=0 HTTP/1.1
Host: 192.168.[redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=7nlr7jlu8jqjcd59rkltq3j8m3
Connection: keep-alive
```

**Command Injection**
A command injection vulnerability is present in the hostname interface of the appliance. A user with the ability to alter the hostname through the web interface may exploit this vulnerability to execute commands as root. The hostname specified in the web interface is written directly to the "/etc/sysconfig/network" file. This file is used by the operating system as part of various commands during startup and shutdown, and additional commands injected via the web interface are run as root. The following set of screenshots shows a set of commands injected into the interface which retrieve and execute a reverse shell binary. The execution is triggered through the web interface by instructing the appliance to shut down or reboot. Brace expansion is used in the example as space characters are stripped from the hostname.

**Proof of Concept**



## Solution

Download the Symantec Web Gateway DB Update v5.0.0.1277 or later.

## Timeline

22/07/2015 – Advisory disclosed to vendor.
23/07/2015 – Vendor acknowledges receipt of advisory.
10/09/2015 – Sent email asking for update.
11/09/2015 – Vendor provides update, states product update and advisory will be released shortly.
17/09/2015 – Vendor releases security advisory.
17/09/2015 – Public advisory release.

## Responsible Disclosure Policy

Security-Assessment.com follows a responsible disclosure policy.

## About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com