Security Advisory
Bosch Rexroth BLADEcontrol-WebVIS

1 Advisory Information

Advisory ID: BOSCH-2016-0701
Published: 22 Jul 2016
Last Updated: 14 Mar 2017
CVSSv3 Base Score:

- SQL Injection: 6.4
- XSS Injection: 6.1

2 Summary

Independent researcher, Maxim Rupp, identified a SQL injection and a cross-site scripting(XSS) vulnerability in Bosch Rexroth BLADEcontrol-WebVIS 3.0.2 and earlier. These vulnerabilities were initially reported by [2]. BLADEcontrol WebVIS is a website used to monitor metrics for wind turbines. It is not used to access or control BLADEcontrol systems or wind turbines itself. Bosch Rexroth has upgraded the website to mitigate these vulnerabilities. New user credentials are required for the new website.

The BLADEcontrol-WebVIS site was vulnerable to a SQL injection vulnerability in which database operations that were unintended by the web application designer could be preformed. These types of attacks, in some instances, can lead to a compromise of the database server or to remote code execution. The BLADEcontrol-WebVIS site was also vulnerable to a XSS vulnerability in which the site failed to validate, filter, or encode user input before returning it to a user's web client. It is possible with the identified vulnerabilities to manipulate and delete data from the databases of the web server including user credentials.

Bosch Rexroth analysis has shown that there was one case where an attacker managed exploit the vulnerability to obtain user credentials consisting of generic user IDs and encrypted passwords. The vulnerable website has been shutdown and the affected accounts were blocked. Further analysis has shown that neither the obtained user credentials were used nor further unauthorised access to the servers occurred.

3 Affected Products

BLADEcontrol-WebVIS, Version 3.0.2 and earlier.

- cpe:/a:rexroth:bladecontrol-webvis:3.0.2 and previous versions

4 Solution

Bosch Rexroth has upgraded the website to WebVIS (v5.4) to mitigate these vulnerabilities. The upgraded website is available at https://webvis.bladecontrol.de.

New credentials must be generated for the website. If you have not already created an account please send an email with your previous username to monitoring.systems@boschrexroth.de and a new account will be generated for you.

5 Vulnerability Details

5.1 SQL Injection Vulnerability

CVE-2016-4507 CVSSv3 Base Score: 6.4
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

5.2 XSS Injection Vulnerability

CVE-2016-4508 CVSSv3 Base Score: 6.1
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

6 Additional Resources

[1] http://bladecontrol.de/
[2] https://ics-cert.us-cert.gov/advisories/ICSA-16-187-01
[3] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4507
[4] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4508

7 Revision History

22 Jul 2016: Initial Publication
14 Mar 2017: Fix Advisory ID