Security Advisory

Honeywell XL Web II Controller Vulnerabilities

Author: Maxim Rupp
February, 2017

Direct references to file or code weaknesses that are mentioned in this advisory will not be disclosed to the public from my side due to ethical reasons. This advisory will be published after patches are available and in agreement with the vendor.

Index

Summary

Overview

The following vulnerabilities refer to the standard web-based configuration interface of the Honeywell XL Web II controller device.

There are currently no known public exploits specifically targeting these vulnerabilities.

Affected Products

The following XL Web II controller versions are affected:

XL20xxBxx, firmware XLWeb2_vUBC_3-04-04-07 and prior, and

CLEA20xxBxx, firmware Eagle_vUBC_3-04-04-07 and prior.

In the CentraLine partner channel, Excel Web II controllers also have been sold under the brand name "EAGLE".

Impact

An unauthenticated, malicious remote user with a low skills would be able to exploit these vulnerabilities.

A malicious user may use these vulnerabilities to expose a password by accessing a specific URL. The XL Web II controller application effectively becomes an entry point into the network where it is located.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture and product implementation.

Background

The affected products, XL Web II controllers, are web-based SCADA systems. According to Honeywell, XL Web II controllers are deployed across several sectors including Critical Manufacturing, Energy, Water and Wastewater Systems, and others. Honeywell estimates that these products are used primarily in Europe and the Middle East.

Identified Security Issues

The following sections list information about the security issues. Please note that findings are not listed by their severity or impact. In addition to this, these findings may also be chained to increase the overall impact.

Path Traversal (CVE-2017-5143**)**

A user without authenticating can make a directory traversal attack by accessing a specific URL. A CVSS v3 base score of 8.6 has been assigned.

Lack of proper sanitization of user-supplied input leads to a Path Traversal vulnerability. The Path Traversal attack technique allows a malicious user to access files that reside outside the web document root directory on the host system.

This vulnerability allows a malicious user to steal sensitive information from the target host which could be used to execute further attacks on the host. For example, to obtain the configuration files.

Access to the affected file was available for users without authentication.

Improper Privilege Management (CVE-2017-5142**)**

A user with low privileges is able to open and change the parameters by accessing a specific URL. A CVSS v3 base score of 9.1 has been assigned.

Users with limited access rights from the "Guest" group or without authentication are denied access to various important functions from a security perspective on the device.

However, it was found that the application does properly restricts access to a resource by an user with limited access rights. A user could still get access to these functions by accessing a specific URL. In such a way, a malicious user could take advantage of those functionalities.

The functions of the following items were affected by this control security weakness:

```
General trend changes
Trend Records Filter
Plants
Control Loops
```

```
Tend records
```

Successful exploitation of this weakness might allow a malicious user to obtain sensitive internal information on the server-side.

Insufficiently Protected Credentials (CVE-2017-5140**) and Plaintext Storage of a Password (**CVE-2017-5139**)**

Any user is able to disclose a password by accessing a specific URL. A CVSS v3 base score of 9.8 has been assigned.
Password is stored in clear text. A CVSS v3 base score of 9.8 has been assigned.

It was discovered that the application stores multiple passwords to access some system functions in JavaScript files in order to make an early verification on client-side, prior to changing the password. In this case the application also stores those credentials in clear text. The existing storage technique for specific passwords could allow malicious user to extract these.

A user was able to access this specific JS files that are responsible for password checking without a valid application session.

At this example the system includes the password of the current *Modem Settings*.

JavaScript code:

```
[SNIP]
if ("remad-1234" != sOldPassword)
        {
          alert ("Wrong Password. Please try again!");
          return;
     }
[SNIP]
```

Therefore, it was possible for a malicious user to discover an actual password from system settings of the application without first logging in.

Mitigation and Solution

Honeywell has developed Version 3.04.05.05 to fix the vulnerabilities in the XL Web II controllers. Users are encouraged to contact the local Honeywell HBS branch to have their sites updated to the latest version (which currently is firmware XLWeb2_vUBC_4-00-00-14).

Controller firmware:
https://www.centraline.com/partnerweb/index.php?id=847&route=article%2Findex&directory_id=190&direct_link=1

CARE programming tool:
https://www.centraline.com/partnerweb/index.php?id=847&route=article%2Findex&directory_id=138&direct_link=1

References

https://ics-cert.us-cert.gov/advisories/ICSA-17-033-01 — Honeywell XL Web II Controller Vulnerabilities

CVE-2017-5139 (CWE-256: Plaintext Storage of a Password)
CVE-2017-5140 (CWE-522: Insufficiently Protected Credentials)
CVE-2017-5141 (CWE-384: Session Fixation)
CVE-2017-5142 (CWE-269: Improper Privilege Management)
CVE-2017-5143 (CWE-23: Relative Path Traversal)

I would like to thank ICS-CERT and Honeywell team for the collaboration and their work during the disclosure and remediation process.