ESA-20180823-01
i.LON 600 Authentication Bypass Flaw

Overview

It is possible to bypass the required authentication specified in the security configuration file by including extra characters in the directory name when specifying the directory to be accessed. Echelon recommends that all i.LON 600s be installed behind a firewall or on a VLAN to minimize exposure to attackers.

Affected Products

All i.LON 600 products.

Vulnerability Overview

Authentication on the i.LON 600 is controlled by configuration directives in the **WebParams.dat** file. When specifying that a particular set of files or directories should be inaccessible without authentication, the path is placed in the configuration file as a string with optional wildcard characters (*) to match zero or more characters. When a Web request is made, the URI must match the entire provided path with wildcards applied, or no authentication will be required. By issuing Web requests with superfluous slashes in the URI (for example, "/forms/////Echelon/SetupSecurity.htm"), the path will not match the one configured to require authentication and will be accessible without any username or password.

Risk Evaluation

The risk is low because this vulnerability cannot be used to access any sensitive information in the i.LON 600. The information that is available is simple configuration information and some performance statistics. While it is possible to read the security web page using this vulnerability, the username and password are both only returned as a series of asterisk characters so it is not possible to use the vulnerability to access the username or password. The risk can be mitigated by installing the i.LON 600 behind a firewall or on a VLAN as described in the next section.

Mitigation

To minimize exposure to attackers, install the i.LON 600 and any servers using the i.LON 600 behind a firewall or on a VLAN without other devices. The VLAN approach limits the threat vector from other internal devices and users that are not part of the same system with the i.LON 600 and associated servers. When using a firewall, to minimize threat exposure do not configure the firewall to do any port forwarding to the i.LON 600.

Acknowledgement

Echelon thanks Maxim Rupp for reporting the vulnerability.

History

V1.0 (2018-08-20): Initial publication