Security Advisory RLCSIM-2023-06
Potential Exploitation of Special Firewall Customization Elements

Product and Version

FlexEdge Gateway

DA50A

DA70A

Crimson 3.2.1028.0 or below

Incidents Covered

RLCSIM-2023-06 – Potential Exploitation of Special Firewall Customization Elements

Abstract and Severity

Authorized users with *Edit Configuration* privileges or greater can change network settings to include special characters that can allow the execution of arbitrary shell instructions.

The vulnerability score is estimated at 7.5 for a rating of HIGH.

For More Information

The Red Lion Security Team can be reached at security-team@redlion.net. For more information on current threats and what we are doing to keep our products and software secure, please visit the link below.

https://support.redlion.net/hc/en-us/categories/360002087671-Security-Advisories

Security Advisory RLCSIM-2023-06
Potential Exploitation of Special Firewall Customization Elements

CVSS v3.1 Vulnerability Score

The vulnerability score is estimated using the link below at 7.5 for a rating of HIGH.

The vector is AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:H/A:H

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Depending on how the device is installed the above score can be modified using the environmental score. For example, the *Modified Attack Vector* element could be set to something other than *Network* in an installation that does not support remote access resulting in a lower score. Similarly, a *Modified Scope* element can be used when writing data to other components of the controls system is not possible or if no significant impact will result.

Hardware Products Affected

FlexEdge Gateway

DA50A

DA70A

Software Versions Affected

Crimson 3.2.1028.0 or below

Vulnerability Details

CWE-138: Improper Neutralization of Special Elements

Embedded products running Red Lion's Crimson 3.2 software prior to version 3.2.1030 contain a vulnerability whereby authorized users with *Edit Configuration* privileges or greater can change network settings to include special characters that can allow the execution of arbitrary shell instructions. These instructions can be used to gain SSH access to the device, or to otherwise compromise its operation.

Solution and Mitigation

The recommended solution is to update the device firmware to that included with Crimson 3.2 version 3.2.1030 or later. This update can be downloaded from the link below.

https://www.redlion.net/support/software-firmware/red-lion-software/crimson

Configuration access to impacted devices should be limited until the software update can be applied.