**Potential Vulnerability**

**CGLine+ connection to CGVision**

<table>
<thead>
<tr>
<th>Date:</th>
<th>Oct 15, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject:</td>
<td>Potential vulnerability with CGLine+ when connected to CGVision</td>
</tr>
<tr>
<td>Severity rating:</td>
<td>High</td>
</tr>
<tr>
<td>Product:</td>
<td>CGLine+ (when connected to CGVision)</td>
</tr>
</tbody>
</table>
| Affected version: | CGLine+ Web Controller: up to version Z1000.H  
CGVision: versions 6.02 to 6.40 |

**General Information**

Eaton performs regular cybersecurity assessments of its applications and implements improvements to security vulnerabilities identified.

Based on these assessments, Eaton is aware of a potential vulnerability in the CGLine+ Web Controller when connected to the supervision software CGVision. This affects all CGLine+ Web Controllers up to software version Z1000.H in combination with the CGVision software version 6.02 up to 6.40. CGLine+ Web Controllers that are not connected to CGVision are not affected.

**Recommendation**

A new version of the CGLine+ Web Controller (Version Z1000.J) is already available. Eaton recommends all customers to install this new software version. Please contact the EATON service hotline (kundendienst@ceag.de or +49 2921 69493) to get the newest firmware.

Another new version of the CGLine+ Web Controller and CGVision software are scheduled for release in November 2019. Customers will be notified immediately of this new release.

For additional information or a list of other issues that have been reported and resolved, please visit our Cybersecurity web site [www.eaton.com/cybersecurity](http://www.eaton.com/cybersecurity), or you can contact us at CybersecurityCOE@eaton.com.

**Best Practices**

Eaton recommends that you follow the best practices listed below when deploying this product. Additional guidelines for securely deploying our products are outlined in our whitepaper, *Cybersecurity Considerations for Electrical Distribution Systems*.

- Always install the latest updates from Eaton
- Protect access to physical ports and cabinets
- Deactivate unused ports/services
- Change passwords regularly
- Always use least privilege
- Whitelist network access if applicable
- Install products in safe environments only as documented

---

Eaton is a registered trademark. All other trademarks are property of their respective owners.