Certain versions of Integrated Lights-out 2 Firmware from Hp contain the following vulnerability:

Unspecified vulnerability in HP Integrated Lights-Out (iLO) firmware 2 before 2.27, 3 before 1.82, and 4 before 2.10 allows remote attackers to bypass intended access restrictions or cause a denial of service via unknown vectors.

CVE-2015-2106 has been assigned by hp-security-alert@hp.com to track the vulnerability.
There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

<table>
<thead>
<tr>
<th>Type</th>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
<th>Update</th>
<th>Edition</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Hp</td>
<td>Integrated Lights-out 2 Firmware</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Operating System</td>
<td>Hp</td>
<td>Integrated Lights-out 3 Firmware</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Operating System</td>
<td>Hp</td>
<td>Integrated Lights-out 4 Firmware</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

No vendor comments have been submitted for this CVE

© CVE.report 2021 ©

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report