Vulnerability Summary
A local privilege-escalation vulnerability exists in the Plantronics Hub for Windows client application. A local attacker can exploit this vulnerability to gain elevated privileges.

CVE-2019-15742

Products Affected
This vulnerability affects Plantronics Hub for Windows prior to version 3.14.

Solution
Poly has released software updates to address this vulnerability.

<table>
<thead>
<tr>
<th>Products</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plantronics Hub for Windows</td>
<td>Update Plantronics Hub for Windows version 3.14 or later</td>
</tr>
</tbody>
</table>


Recognition
Poly appreciates and values the members of the security research community who find vulnerabilities, bring them to our attention, and work with Poly in a coordinated effort so that security fixes can be issued to all impacted customers. We would like to thank security researcher Markus Krell from NTT Ltd. for discovering this vulnerability, alerting us, and for his cooperative disclosure.

CVSS v3 Base Metrics
To assist our customers in the evaluation of this vulnerability, Poly uses the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v3 Scores
For more information on CVSS v3 please see: https://www.first.org/cvss

Severity: High

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.</td>
</tr>
<tr>
<td>High</td>
<td>A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.</td>
</tr>
<tr>
<td>Medium</td>
<td>A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.</td>
</tr>
<tr>
<td>Low</td>
<td>A vulnerability that has minimal impact to the system and is extremely difficult to exploit.</td>
</tr>
</tbody>
</table>

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Poly Technical Support – either call 1-800-POLYCOM or visit:

https://support.polycom.com/content/support/security-center.html For the latest information.

You might also find value in the high-level security guidance and security news located at:

https://support.polycom.com/content/support/security-center.html

Revision History

Revision 1.0 - Original publication: August 30, 2019
consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Poly has been advised of the possibility of such damages.