



# CVE-2012-6611

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2012-6611   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2020-02-10 15:15:00 UTC   |
| <b>Updated</b>         | 2020-02-14 15:42:00 UTC   |
| <b>Description</b>     | An issue was discovered in Polycom Web Management Interface G3/HDX 8000 HD with Durango 2.6.0 4740 software and |

## Risk And Classification

**Problem Types:** CWE-798

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor                  | Product                  | Version | Update | Edition | Language |
|----------|-------------------------|--------------------------|---------|--------|---------|----------|
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 4002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 4002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 4500</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 4500</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 6000</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 6000</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 7001</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 7001</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 7002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 7002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8002</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8004</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8004</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8006</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 8006</a> | -       | All    | All     | All      |
| Hardware | <a href="#">Polycom</a> | <a href="#">Hdx 9002</a> | -       | All    | All     | All      |

|             |                         |                                     |     |     |     |     |
|-------------|-------------------------|-------------------------------------|-----|-----|-----|-----|
| Hardware    | <a href="#">Polycom</a> | <a href="#">Hdx 9002</a>            | -   | All | All | All |
| Hardware    | <a href="#">Polycom</a> | <a href="#">Hdx 9004</a>            | -   | All | All | All |
| Hardware    | <a href="#">Polycom</a> | <a href="#">Hdx 9004</a>            | -   | All | All | All |
| Hardware    | <a href="#">Polycom</a> | <a href="#">Hdx 9006</a>            | -   | All | All | All |
| Hardware    | <a href="#">Polycom</a> | <a href="#">Hdx 9006</a>            | -   | All | All | All |
| Application | <a href="#">Polycom</a> | <a href="#">Hdx System Software</a> | All | All | All | All |

## References

| Reference  | Source  | Link   | Tags         |
|--|---------|--|--------------|
| Polycom - Command Shell Authorization Bypass (Metasploit) - Unix remote Exploit        | MISC    | <a href="http://www.exploit-db.com">www.exploit-db.com</a> | Exploit, ... |
| João Paulo Campello: Path Traversal on Polycom Web Management Interface - Tempest Blog | MISC    | <a href="http://web.archive.org">web.archive.org</a>       | Exploit, ... |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>               | canonical    |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>             | canonical    |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](https://status.cve.report)