



# CVE-2018-16158

Published on: 08/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

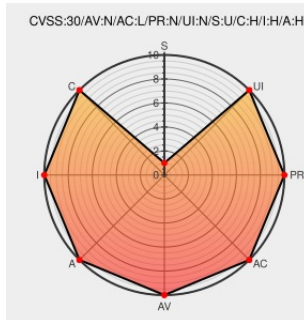
## CVE-2018-16158

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Power Xpert Meter 4000** from **Eaton** contain the following vulnerability:

Eaton Power Xpert Meter 4000, 6000, and 8000 devices before 13.4.0.10 have a single SSH private key across different customers' installations and do not properly restrict access to this key, which makes it easier for remote attackers to perform SSH logins (to uid 0) via the PubkeyAuthentication option.

CVE-2018-16158 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **10 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description | Tags                                                                                                | Link                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|             | <a href="#">Vendor Advisory</a><br><a href="#">www.eaton.com</a><br><a href="#">application/pdf</a> | <a href="#">MISC www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/PXM-Advisory.pdf</a> |

msf/eaton\_known\_privkey.rb at master · BrianWGray/msf · GitHub

Exploit

Third Party Advisory

github.com

text/html

 MISC  
github.com/BrianWGray/msf/blob/master/exploits/linux/ssh/eaton\_known\_privkey.rb

Something Broken - CTRLu.Net

Exploit

Third Party Advisory

www.ctrlu.net

text/html

 MISC [www.ctrlu.net/vuln/0006.html](http://www.ctrlu.net/vuln/0006.html)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

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

| Type                                                                                         | Vendor | Product                                         | Version | Update | Edition | Language |
|----------------------------------------------------------------------------------------------|--------|-------------------------------------------------|---------|--------|---------|----------|
| Hardware    | Eaton  | <a href="#">Power Xpert Meter 4000</a>          | -       | All    | All     | All      |
| Hardware    | Eaton  | <a href="#">Power Xpert Meter 4000</a>          | -       | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 4000 Firmware</a> | All     | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 4000 Firmware</a> | All     | All    | All     | All      |
| Hardware  | Eaton  | <a href="#">Power Xpert Meter 6000</a>          | -       | All    | All     | All      |
| Hardware  | Eaton  | <a href="#">Power Xpert Meter 6000</a>          | -       | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 6000 Firmware</a> | All     | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 6000 Firmware</a> | All     | All    | All     | All      |
| Hardware  | Eaton  | <a href="#">Power Xpert Meter 8000</a>          | -       | All    | All     | All      |
| Hardware  | Eaton  | <a href="#">Power Xpert Meter 8000</a>          | -       | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 8000 Firmware</a> | All     | All    | All     | All      |
| Operating System                                                                             | Eaton  | <a href="#">Power Xpert Meter 8000 Firmware</a> | All     | All    | All     | All      |

cpe:2.3:h:eaton:power\_xpert\_meter\_4000:-:\*:\*:\*:\*:\*:

cpe:2.3:h:eaton:power\_xpert\_meter\_4000:-:\*:\*:\*:\*:\*:

cpe:2.3:o:eaton:power\_xpert\_meter\_4000\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:eaton:power\_xpert\_meter\_4000\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:h:eaton:power\_xpert\_meter\_6000:-:\*:\*:\*:\*:\*:

|                                                        |
|--------------------------------------------------------|
| cpe:2.3:h:eaton:power_xpert_meter_6000:-:*****:        |
| cpe:2.3:o:eaton:power_xpert_meter_6000_firmware:*****: |
| cpe:2.3:o:eaton:power_xpert_meter_6000_firmware:*****: |
| cpe:2.3:h:eaton:power_xpert_meter_8000:-:*****:        |
| cpe:2.3:h:eaton:power_xpert_meter_8000:-:*****:        |
| cpe:2.3:o:eaton:power_xpert_meter_8000_firmware:*****: |
| cpe:2.3:o:eaton:power_xpert_meter_8000_firmware:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)