



# CVE-2016-9347

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

## Summary

|                        |                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-9347                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                         |
| <b>Assigner</b>        | ics-cert@hq.dhs.gov                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                   |
| <b>Published</b>       | 2017-02-13 21:59:00 UTC                                                                                        |
| <b>Updated</b>         | 2017-03-13 16:52:00 UTC                                                                                        |
| <b>Description</b>     | An issue was discovered in Emerson SE4801T0X Redundant Wireless I/O Card V13.3, and SE4801T1X Simplex Wireless |

## Risk And Classification

**Problem Types:** CWE-254

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                  | Product                                                        | Version | Update | Edition | Language |
|------------------|-------------------------|----------------------------------------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card Firmware</a> | 13.3    | All    | All     | All      |
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card Firmware</a> | 13.3    | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t0x Redundant Wireless I/o Card Firmware</a> | 13.3    | All    | All     | All      |
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card</a>            | -       | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card Firmware</a>   | 13.3    | All    | All     | All      |
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card</a>            | -       | All    | All     | All      |
| Hardware         | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card</a>            | -       | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card Firmware</a>   | 13.3    | All    | All     | All      |
| Operating System | <a href="#">Emerson</a> | <a href="#">Se4801t1x Simplex Wireless I/o Card Firmware</a>   | 13.3    | All    | All     | All      |

## References

| Reference                                                               | Source | Link                                                             | Tags                    |
|-------------------------------------------------------------------------|--------|------------------------------------------------------------------|-------------------------|
| Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability   ICS-CERT | MISC   | <a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>  | Third Party Advisory, U |
| Multiple Emerson Products CVE-2016-9347 Security Bypass Vulnerability   | BID    | <a href="http://www.securityfocus.com">www.securityfocus.com</a> | Third Party Advisory, V |

|                                                                                      |         |                                                |                     |
|--------------------------------------------------------------------------------------|---------|------------------------------------------------|---------------------|
| 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, analysis |
| <div> <div></div> <div></div> </div>                                                 |         |                                                |                     |
| No vendor comments have been submitted for this CVE.                                 |         |                                                |                     |
| Legacy QID Mappings                                                                  |         |                                                |                     |
| 590585 Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability (ICSA-16-334-03) |         |                                                |                     |

© [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 registred 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](#).
   
**Free CVE JSON API** [cve.report/api](http://cve.report/api)
  
**CVE.report and Source URL Uptime Status** [status.cve.report](#)