



# CVE-2013-2566

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2013-2566   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2013-03-15 21:55:00 UTC   |
| <b>Updated</b>         | 2020-11-23 19:48:00 UTC   |
| <b>Description</b>     | The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for r |

## Risk And Classification

**Problem Types:** CWE-326

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                         | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 12.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 13.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 13.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 12.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 13.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 13.10   | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-1</a>           | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-1</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a>   | <a href="#">M10-1 Firmware</a>  | All     | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a>   | <a href="#">M10-1 Firmware</a>  | All     | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-4</a>           | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-4</a>           | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-4s</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Fujitsu</a>   | <a href="#">M10-4s</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Fujitsu</a>   | <a href="#">M10-4s Firmware</a> | All     | All    | All     | All      |

|                  |         |   |            |     |     |     |
|------------------|---------|---|------------|-----|-----|-----|
| Operating System | Fujitsu | M10-4s Firmware                               | All        | All | All | All |
| Operating System | Fujitsu | M10-4 Firmware                                | All        | All | All | All |
| Operating System | Fujitsu | M10-4 Firmware                                | All        | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M3000                        | -          | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M3000                        | -          | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M3000 Firmware               | All        | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M3000 Firmware               | All        | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M4000                        | -          | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M4000                        | -          | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M4000 Firmware               | All        | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M4000 Firmware               | All        | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M5000                        | -          | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M5000                        | -          | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M5000 Firmware               | All        | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M5000 Firmware               | All        | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M8000                        | -          | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M8000                        | -          | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M8000 Firmware               | All        | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M8000 Firmware               | All        | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M9000                        | -          | All | All | All |
| Hardware         | Fujitsu | Sparc Enterprise M9000                        | -          | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M9000 Firmware               | All        | All | All | All |
| Operating System | Fujitsu | Sparc Enterprise M9000 Firmware               | All        | All | All | All |
| Application      | Mozilla | Firefox                                       | All        | All | All | All |
| Application      | Mozilla | Firefox                                       | All        | All | All | All |
| Application      | Mozilla | Firefox Esr                                   | All        | All | All | All |
| Application      | Mozilla | Firefox Esr                                   | All        | All | All | All |
| Application      | Mozilla | Seamonkey                                     | All        | All | All | All |
| Application      | Mozilla | Seamonkey                                     | All        | All | All | All |
| Application      | Mozilla | Thunderbird                                   | All        | All | All | All |
| Application      | Mozilla | Thunderbird                                   | All        | All | All | All |
| Application      | Mozilla | Thunderbird Esr                               | All        | All | All | All |
| Application      | Mozilla | Thunderbird Esr                               | All        | All | All | All |
| Application      | Oracle  | Communications Application Session Controller | All        | All | All | All |
| Application      | Oracle  | Http Server                                   | 11.1.1.7.0 | All | All | All |

|                  |        |  |            |     |     |     |
|------------------|--------|--|------------|-----|-----|-----|
| Application      | Oracle | Http Server                            | 11.1.1.9.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.1.3.0.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.2.1.1.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.2.1.2.0 | All | All | All |
| Application      | Oracle | Http Server                            | 11.1.1.7.0 | All | All | All |
| Application      | Oracle | Http Server                            | 11.1.1.9.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.1.3.0.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.2.1.1.0 | All | All | All |
| Application      | Oracle | Http Server                            | 12.2.1.2.0 | All | All | All |
| Operating System | Oracle | Integrated Lights Out Manager Firmware | All        | All | All | All |
| Operating System | Oracle | Integrated Lights Out Manager Firmware | All        | All | All | All |

## References

| Reference   | Source  | Link   |
|---|---------|--|
| Oracle Critical Patch Update Advisory - April 2016  | CONFIRM | <a href="http://www.oracle.com">www.oracle.com</a>               |
| Welcome - Opera Security Corner   | CONFIRM | <a href="http://www.opera.com">www.opera.com</a>                 |
| SSL/TLS RC4 CVE-2013-2566 Information Disclosure Weakness   | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a> |
| Oracle Critical Patch Update - July 2016  | CONFIRM | <a href="http://www.oracle.com">www.oracle.com</a>               |
| Document Display   HPE Support Center   | CONFIRM | <a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>       |
| MFSA 2013-103: Miscellaneous Network Security Services (NSS) vulnerabilities                                  | CONFIRM | <a href="http://www.mozilla.org">www.mozilla.org</a>             |
| <a href="http://cr.yip.to/talks/2013.03.12/slides.pdf">cr.yip.to/talks/2013.03.12/slides.pdf</a>              | MISC    | <a href="http://cr.yip.to">cr.yip.to</a>                         |
| USN-2032-1: Thunderbird vulnerabilities   Ubuntu  | UBUNTU  | <a href="http://www.ubuntu.com">www.ubuntu.com</a>               |
| Gentoo Security   | GENTOO  | <a href="http://security.gentoo.org">security.gentoo.org</a>     |
| Oracle Critical Patch Update - January 2018   | CONFIRM | <a href="http://www.oracle.com">www.oracle.com</a>               |
| Oracle Critical Patch Update - October 2016   | CONFIRM | <a href="http://www.oracle.com">www.oracle.com</a>               |
| The Opera Security group - On the Precariousness of RC4   | CONFIRM | <a href="http://my.opera.com">my.opera.com</a>                   |
| '[security bulletin] HPSBGN03324 rev.1 - HP Business Service Automation Essentials Core, Remote Discl' - MARC | HP      | <a href="http://marc.info">marc.info</a>                         |
| Document Display   HPE Support Center   | CONFIRM | <a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>       |
| Gentoo Linux Documentation -- Mozilla Network Security Service: Multiple vulnerabilities                      | GENTOO  | <a href="http://security.gentoo.org">security.gentoo.org</a>     |
| On the Security of RC4 in TLS   | MISC    | <a href="http://www.isg.rhcloud.com">www.isg.rhcloud.com</a>     |
| A Few Thoughts on Cryptographic Engineering: Attack of the week: RC4 is kind of broken in TLS                 | MISC    | <a href="http://blog.cryptologic.com">blog.cryptologic.com</a>   |
| USN-2031-1: Firefox vulnerabilities   Ubuntu  | UBUNTU  | <a href="http://www.ubuntu.com">www.ubuntu.com</a>               |
| Opera for Mobile Devices  | CONFIRM | <a href="http://www.opera.com">www.opera.com</a>                 |
| Oracle Critical Patch Update - October 2017   | CONFIRM | <a href="http://www.oracle.com">www.oracle.com</a>               |
| Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView                    | CONFIRM | <a href="http://kb.juniper.net">kb.juniper.net</a>               |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                     |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

591186 Mitsubishi Electric Air Conditioning Systems Multiple Vulnerabilities (ICSA-22-160-01)

© [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](#)