



# CVE-2016-7553

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-7553                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | security@debian.org                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2017-02-27 22:59:00 UTC                                                                                                   |
| <b>Updated</b>         | 2023-11-07 02:34:00 UTC                                                                                                   |
| <b>Description</b>     | The buf.pl script before 2.20 in Irssi before 0.8.20 uses weak permissions for the scrollbar dump file created between up |

## Risk And Classification

### Problem Types: CWE-275

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                | Product                | Version | Update | Edition | Language |
|-------------|-----------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Irssi</a> | <a href="#">Buf.pl</a> | All     | All    | All     | All      |

## References

| Reference                                                                                  | Source  | Link                                    | Tags   |
|--------------------------------------------------------------------------------------------|---------|-----------------------------------------|--------|
| <a href="#">irssi.org/security/buf_pl_sa_2016.txt</a>                                      | CONFIRM | <a href="#">irssi.org</a>               | Patch  |
| [SECURITY] Fedora 25 Update: irssi-0.8.20-2.fc25 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="#">lists.fedoraproject.org</a> | Third  |
| Fix disclosure via filesystem · irssi/scripts.irssi.org@f1b1eb1 · GitHub                   | CONFIRM | <a href="#">github.com</a>              | Patch  |
| Irssi 'buf.pl' Local Information Disclosure Vulnerability                                  | BID     | <a href="#">www.securityfocus.com</a>   | Third  |
| oss-security - CVE Request: irssi: information disclosure vulnerabilit in buf.pl           | MLIST   | <a href="#">www.openwall.com</a>        | Mailir |
| oss-security - Re: CVE Request: irssi: information disclosure vulnerabilit in buf.pl       | MLIST   | <a href="#">www.openwall.com</a>        | Mailir |
| [SECURITY] Fedora 25 Update: irssi-0.8.20-2.fc25 - package-announce - Fedora Mailing-Lists |         | <a href="#">lists.fedoraproject.org</a> |        |
| CVE Program record                                                                         | CVE.ORG | <a href="#">www.cve.org</a>             | canon  |
| NVD vulnerability detail                                                                   | NVD     | <a href="#">nvd.nist.gov</a>            | canon  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[670274](#) EulerOS Security Update for irssi (EulerOS-SA-2021-1803)

[670901](#) EulerOS Security Update for irssi (EulerOS-SA-2021-1306)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)