



CVE-2018-11780

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-11780 |
| State | PUBLIC |
| Assigner | security@apache.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-09-17 14:29:00 UTC |
| Updated | 2023-11-07 02:51:00 UTC |
| Description | A potential Remote Code Execution bug exists with the PDFInfo plugin in Apache SpamAssassin before 3.4.2. |

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------------|------------------------------|---------|--------|---------|----------|
| Application | Apache | Spamassassin | All | All | All | All |
| Application | Apache | Spamassassin | All | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Pdfinfo Project | Pdfinfo | - | All | All | All |
| Application | Pdfinfo Project | Pdfinfo | - | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------------------------------|--|----------------------|
| SpamAssassin: Multiple vulnerabilities (GLSA 201812-07) | Gentoo security | GENTOO security.gentoo.org | Third Party Advisory |

| | | | |
|---|---------|---|---------------------------|
| SpamAssassin: multiple vulnerabilities (GLSA 201812-07) — Gentoo Security | GENTOO | security.gentoo.org | Third Party Advisory |
| USN-3811-1: SpamAssassin vulnerabilities Ubuntu security notices | UBUNTU | usn.ubuntu.com | Third Party Advisory |
| Apache Mail Archives | MLIST | lists.apache.org | Mailing List, Mitigation |
| Apache SpamAssassin CVE-2018-11780 Remote Code Execution Vulnerability | BID | www.securityfocus.com | Third Party Advisory |
| Apache Mail Archives | | lists.apache.org | |
| USN-3811-3: SpamAssassin vulnerabilities Ubuntu security notices | UBUNTU | usn.ubuntu.com | Third Party Advisory |
| [security-announce] openSUSE-SU-2019:1831-1: moderate: Security update f | SUSE | lists.opensuse.org | |
| [SECURITY] [DLA 1578-1] spamassassin security update | MLIST | lists.debian.org | Mailing List, Third Party |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [500642](#) Alpine Linux Security Update for spamassassin
- [504409](#) Alpine Linux Security Update for spamassassin
- [710244](#) Gentoo Linux SpamAssassin Multiple Vulnerabilities (GLSA 201812-07)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report