# CVE-2013-0288

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2013-0288 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2013-03-05 21:38:55 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | nss-pam-ldapd before 0.7.18 and 0.8.x before 0.8.11 allows context-dependent attackers to cause a denial of service (appli |

## Risk And Classification

**Primary CVSS:** v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

**Problem Types:** CWE-119 | n/a

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Arthurdejong | Nss-pam-ldapd | 0.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Arthurdejong | Nss-pam-ldapd | 0.2 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.2.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.3 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.4 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.4.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.5 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.0 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.10 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.11 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.12 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.2 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.3 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.4 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.5 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.6 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.7 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.7.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.7.2 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.8 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.6.9 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.0 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.10 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.11 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.12 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.13 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.14 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.15 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.16 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.2 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.3 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.4 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.5 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.6 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.7 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.8 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.7.9 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.0 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.1 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.10 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.2 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.3 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.4 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.5 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.6 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.7 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.8 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | 0.8.9 | All | All | All |
| Application | Arthurdejong | Nss-pam-ldapd | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source |
|---|---|
| Security Advisory SA52212 - nss-pam-ldapd File Descriptor Handling Buffer Overflow Vulnerability - Secunia | af854a3a-21 |
| Support / Security / Advisories / / MDVSA-2013:106 \| Mandriva | af854a3a-21 |
| Red Hat Customer Portal | af854a3a-21 |
| nss-pam-ldapd 'FD_SET()' Function Stack Buffer Overflow Vulnerability | af854a3a-21 |
| 909119 – (CVE-2013-0288) CVE-2013-0288 nss-pam-ldapd: FD_SET array index error, leading to stack-based buffer overflow | af854a3a-21 |
| openSUSE-SU-2013:0522-1: moderate: nss-pam-ldapd: fixed FD_SET overflow | af854a3a-21 |
| IBM X-Force Exchange | af854a3a-21 |
| nss-pam-ldapd - NSS and PAM modules for lookups using LDAP | af854a3a-21 |
| [SECURITY] Fedora 17 Update: nss-pam-ldapd-0.7.16-3.fc17 | af854a3a-21 |
| nss-pam-ldapd - NSS and PAM modules for lookups using LDAP | af854a3a-21 |
| #690319 - lookup fail to contact nslcd when first 1024 filedescriptor are already used (select) - Debian Bug report logs | af854a3a-21 |
| openSUSE-SU-2013:0524-1: moderate: nss-pam-ldapd: fixed FD_SET overflow | af854a3a-21 |
| Support/Advisories/MGASA-2013-0071 - Mageia wiki | af854a3a-21 |
| Security Advisory SA52242 - Debian update for nss-pam-ldapd - Secunia | af854a3a-21 |

| | |
|---|---|
| Debian -- Page not found | af854a3a-21 |
| oss-security - CVE-2013-0288 nss-pam-ldapd: FD_SET array index error, leading to stack-based buffer overflow | af854a3a-21 |
| nss-pam-ldapd - NSS and PAM modules for lookups using LDAP | af854a3a-21 |
| nss-pam-ldapd security advisory (CVE-2013-0288) | af854a3a-21 |
| Red Hat Customer Portal | MITRE |
| access.redhat.com \| CVE-2013-0288 | MITRE |
| Bug 909119 – CVE-2013-0288 nss-pam-ldapd: FD_SET array index error, leading to stack-based buffer overflow | MITRE |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.