



# CVE-2012-0038

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

| Summary         |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2012-0038                                                                                                                    |
| State           | PUBLISHED                                                                                                                        |
| Assigner        | redhat                                                                                                                           |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                     |
| Published       | 2012-05-17 11:00:35 UTC                                                                                                          |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                          |
| Description     | Integer overflow in the xfs_acl_from_disk function in fs/xfs/xfs_acl.c in the Linux kernel before 3.1.9 allows local users to ca |

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-190 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov | Primary | 5.5   | MEDIUM   | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| 2.0     | nvd@nist.gov | Primary | 4.9   |          | AV:L/AC:L/Au:N/C:N/I:N/A:C                   |

| CVSS v3.1 Breakdown |           |
|---------------------|-----------|
| Attack Vector       | Local     |
| Attack Complexity   | Low       |
| Privileges Required | Low       |
| User Interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | None      |
| Integrity           | None      |
| Availability        |           |

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:N/A:C

| NVD Known Affected Configurations (CPE 2.3) |        |              |         |        |         |          |
|---------------------------------------------|--------|--------------|---------|--------|---------|----------|
| Type                                        | Vendor | Product      | Version | Update | Edition | Language |
| Operating System                            | Linux  | Linux Kernel | 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                               | Link        |  |
| www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1.9                                   | af854a3a-2127-422b-91ae-364da2661108 | www.kern    |  |
| xfs: fix acl count validation in xfs_acl_from_disk() · torvalds/linux@093019c · GitHub | af854a3a-2127-422b-91ae-364da2661108 | github.cor  |  |
| oss-security - Re: CVE request: kernel: xfs heap overflow                              | af854a3a-2127-422b-91ae-364da2661108 | www.oper    |  |
| 773280 – (CVE-2012-0038) CVE-2012-0038 kernel: xfs heap overflow                       | af854a3a-2127-422b-91ae-364da2661108 | bugzilla.re |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                               | af854a3a-2127-422b-91ae-364da2661108 | git.kernel. |  |
| xfs: validate acl count · torvalds/linux@fa8b18e · GitHub                              | af854a3a-2127-422b-91ae-364da2661108 | github.cor  |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                               | af854a3a-2127-422b-91ae-364da2661108 | git.kernel. |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                               | MITRE                                | git.kernel. |  |
| kernel/git/torvalds/linux.git - Linux kernel source tree                               | MITRE                                | git.kernel. |  |
| CVE Program record                                                                     | CVE.ORG                              | www.cve.    |  |

No vendor comments have been submitted for this CVE.

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

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

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

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)