# CVE-2017-1000112

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-1000112 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-10-05 01:29:00 UTC |
| **Updated** | 2023-06-07 12:46:00 UTC |
| **Description** | Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_I |

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Linux Kernel - UDP Fragmentation Offset 'UFO' Privilege Escalation (Metasploit) - Linux local Exploit | EXPLOIT-DB | www |
| Red Hat Customer Portal | REDHAT | acces |
| Linux Kernel UDP Fragmentation Offload Race Condition Lets Local Users Gain Elevated Privileges - SecurityTracker | SECTRACK | www |
| Malformed Request | BID | www |
| Red Hat Customer Portal | REDHAT | acces |
| Red Hat Customer Portal | REDHAT | acces |
| kernel-exploits/CVE-2017-1000112 at master · xairy/kernel-exploits · GitHub | MISC | githu |
| Red Hat Customer Portal | REDHAT | acces |
| Red Hat Customer Portal | REDHAT | acces |
| Red Hat Customer Portal | REDHAT | acces |
| Debian -- Security Information -- DSA-3981-1 linux | DEBIAN | www |
| Red Hat Customer Portal | REDHAT | acces |

| | | |
|---|---|---|
| oss-sec: Linux kernel: CVE-2017-1000112: Exploitable memory corruption due to UFO to non-UFO path switch | MLIST | seclis |
| CVE Program record | CVE.ORG | www |
| NVD vulnerability detail | NVD | nvd.r |

No vendor comments have been submitted for this CVE.

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

© 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 registred 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**