# CVE-2002-0639

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2002-0639 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2002-07-03 04:00:00 UTC |
| **Updated** | 2025-04-03 01:03:51 UTC |
| **Description** | Integer overflow in sshd in OpenSSH 2.9.9 through 3.3 allows remote attackers to execute arbitrary code during challenge r |

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

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

**Problem Types:** CWE-190 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 10 | | AV:N/AC:L/Au:N/C:C/I:C/A:C |

## CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Openbsd | Openssh | All | All | All | All |

## Vendor Declared Affected Products

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

## References

| Reference |
|---|
| Neohapsis Archives - Bugtraq - [OpenPKG-SA-2002.005] OpenPKG Security Advisory (openssh) - From openpkgopenpkg.org |
| 'How to reproduce OpenSSH Overflow.' - MARC |
| www.osvdb.org/6245 |
| Anytime na Twitterze: "There are a lot of redactions here, but it looks like the focus here might have been an exploit that lead also to the follow |
| Debian -- Security Information -- DSA-134-4 ssh |
| ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-030.0.txt |
| CERT Advisory CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling |
| OpenSSH Challenge-Response Buffer Overflow Vulnerabilities |
| Home - Conectiva |
| LinuxSecurity.com: EnGarde: OpenSSH vulnerabilities |

| |
|---|
| Mandrakesoft Security Advisories |
| www1.itrc.hp.com/service/cki/docDisplay.do |
| ISS X-Force Database: openssh-challenge-response-bo (9169): OpenSSH "Challenge-Response" authentication buffer overflow |
| advise123 |
| CERT/CC Vulnerability Note VU#369347 |
| 'OpenSSH Security Advisory (adv.iss)' - MARC |
| 'Revised OpenSSH Security Advisory (adv.iss)' - MARC |
| CVE Program record |
| NVD vulnerability detail |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Red Hat | 2008-05-15 | Mark J Cox | Not vulnerable. This issue did not affect the versions of OpenSSH as shipped with Red Hat Ente |

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