# CVE-2002-0640

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2002-0640 |
| **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** | Buffer overflow in sshd in OpenSSH 2.3.1 through 3.3 may allow remote attackers to execute arbitrary code via a large num |

## Risk And Classification

**Primary CVSS:** v2.0 10 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

### 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 | 1.2.2 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Openbsd | Openssh | 1.2.3 | All | All | All |
| Application | Openbsd | Openssh | 2.1 | All | All | All |
| Application | Openbsd | Openssh | 2.1.1 | All | All | All |
| Application | Openbsd | Openssh | 2.2 | All | All | All |
| Application | Openbsd | Openssh | 2.3 | All | All | All |
| Application | Openbsd | Openssh | 2.5 | All | All | All |
| Application | Openbsd | Openssh | 2.5.1 | All | All | All |
| Application | Openbsd | Openssh | 2.5.2 | All | All | All |
| Application | Openbsd | Openssh | 2.9 | All | All | All |
| Application | Openbsd | Openssh | 2.9.9 | All | All | All |
| Application | Openbsd | Openssh | 2.9p1 | All | All | All |
| Application | Openbsd | Openssh | 2.9p2 | All | All | All |
| Application | Openbsd | Openssh | 3.0 | All | All | All |
| Application | Openbsd | Openssh | 3.0.1 | All | All | All |
| Application | Openbsd | Openssh | 3.0.1p1 | All | All | All |
| Application | Openbsd | Openssh | 3.0.2 | All | All | All |
| Application | Openbsd | Openssh | 3.0.2p1 | All | All | All |
| Application | Openbsd | Openssh | 3.0p1 | All | All | All |
| Application | Openbsd | Openssh | 3.1 | All | All | All |
| Application | Openbsd | Openssh | 3.1p1 | All | All | All |
| Application | Openbsd | Openssh | 3.2 | All | All | All |
| Application | Openbsd | Openssh | 3.2.2p1 | All | All | All |
| Application | Openbsd | Openssh | 3.2.3p1 | All | All | All |
| Application | Openbsd | Openssh | 3.3 | All | All | All |
| Application | Openbsd | Openssh | 3.3p1 | 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 |
|---|---|---|
| redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.r |
| 'Sun statement on the OpenSSH Remote Challenge Vulnerability' - MARC | af854a3a-2127-422b-91ae-364da2661108 | marc.i |
| www.osvdb.org/839 | af854a3a-2127-422b-91ae-364da2661108 | www.o |
| 'How to reproduce OpenSSH Overflow.' - MARC | af854a3a-2127-422b-91ae-364da2661108 | marc.i |
| www.openwall.com/lists/oss-security/2024/07/01/2 | af854a3a-2127-422b-91ae-364da2661108 | www.o |

| | | |
|---|---|---|
| www.openwall.com/lists/oss-security/2024/07/01/3 | af854a3a-2127-422b-91ae-364da2661108 | www.c |
| redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.r |
| Debian -- Security Information -- DSA-134-4 ssh | af854a3a-2127-422b-91ae-364da2661108 | www.c |
| ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-030.0.txt | af854a3a-2127-422b-91ae-364da2661108 | ftp.cal |
| CERT Advisory CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling | af854a3a-2127-422b-91ae-364da2661108 | www.c |
| OpenSSH Challenge-Response Buffer Overflow Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | www.s |
| Home - Conectiva | af854a3a-2127-422b-91ae-364da2661108 | distro. |
| LinuxSecurity.com: EnGarde: OpenSSH vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | www.li |
| 404 Page Not Found \| SUSE | af854a3a-2127-422b-91ae-364da2661108 | www.r |
| Mandrakesoft Security Advisories | af854a3a-2127-422b-91ae-364da2661108 | www.r |
| www1.itrc.hp.com/service/cki/docDisplay.do | af854a3a-2127-422b-91ae-364da2661108 | www1 |
| CERT/CC Vulnerability Note VU#369347 | af854a3a-2127-422b-91ae-364da2661108 | www.k |
| 'OpenSSH Security Advisory (adv.iss)' - MARC | af854a3a-2127-422b-91ae-364da2661108 | marc.i |
| 'Revised OpenSSH Security Advisory (adv.iss)' - MARC | af854a3a-2127-422b-91ae-364da2661108 | marc.i |
| CVE Program record | CVE.ORG | www.c |
| NVD vulnerability detail | NVD | nvd.ni |

No vendor comments have been submitted for this CVE.

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