



# CVE-2001-0249

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

## Summary

|                 |                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2001-0249                                                                                                           |
| State           | PUBLISHED                                                                                                               |
| Assigner        | mitre                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                            |
| Published       | 2001-06-18 04:00:00 UTC                                                                                                 |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                 |
| Description     | Heap overflow in FTP daemon in Solaris 8 allows remote attackers to execute arbitrary commands by creating a long pathn |

## 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-131 | 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 |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | Hp     | Hp-ux   | 11.00   | All    | All     | All      |
| Operating System | Oracle | Solaris | 8       | All    | All     | All      |
| Operating System | Sgi    | Irix    | 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                                                                           |
|-------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------|
| Solaris ftpd glob() Expansion LIST Heap Overflow Vulnerability                | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.securityexchange.org">www.securityexchange.org</a>         |
| IBM X-Force Exchange                                                          | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |
| Network Associates - Research - COVERT                                        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.nai.com">www.nai.com</a>                                   |
| CERT Advisory CA-2001-07 File Globbing Vulnerabilities in Various FTP Servers | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.cert.org">www.cert.org</a>                                 |
| CVE Program record                                                            | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>                                   |
| NVD vulnerability detail                                                      | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                 |

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 registered 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](#)