



# CVE-2001-0797

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2001-0797                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2001-12-12 05:00:00 UTC                                                                                                    |
| <b>Updated</b>         | 2018-10-30 16:26:00 UTC                                                                                                    |
| <b>Description</b>     | Buffer overflow in login in various System V based operating systems allows remote attackers to execute arbitrary commands |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor              | Product               | Version | Update | Edition | Language |
|------------------|---------------------|-----------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.00   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.01   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.10   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.20   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.24   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.0.4  | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.00   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.11   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.00   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.01   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.10   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.20   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 10.24   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.0.4  | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.00   | All    | All     | All      |
| Operating System | <a href="#">Hp</a>  | <a href="#">Hp-ux</a> | 11.11   | All    | All     | All      |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>   | 4.3     | All    | All     | All      |

|                  |                     |                            |        |     |     |     |
|------------------|---------------------|----------------------------|--------|-----|-----|-----|
|                  |                     |                            |        |     |     |     |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.1  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.2  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.3  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 5.1    | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3    | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.1  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.2  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 4.3.3  | All | All | All |
| Operating System | <a href="#">Ibm</a> | <a href="#">Aix</a>        | 5.1    | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0    | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.1  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.2  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.3  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.4  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.5  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.6  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.6a | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0    | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.1  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.2  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.3  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.4  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.5  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.6  | All | All | All |
| Operating System | <a href="#">Sco</a> | <a href="#">Openserver</a> | 5.0.6a | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.2    | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3    | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.1  | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.2  | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.3  | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.2    | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3    | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.1  | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.2  | All | All | All |
| Operating System | <a href="#">Sgi</a> | <a href="#">Irix</a>       | 3.3.3  | All | All | All |

|                  |     |         |       |     |     |     |
|------------------|-----|---------|-------|-----|-----|-----|
| Operating System | Sun | Solaris | 2.4   | All | x86 | All |
| Operating System | Sun | Solaris | 2.5   | All | x86 | All |
| Operating System | Sun | Solaris | 2.5.1 | All | ppc | All |
| Operating System | Sun | Solaris | 2.5.1 | All | x86 | All |
| Operating System | Sun | Solaris | 2.6   | All | All | All |
| Operating System | Sun | Solaris | 7.0   | All | x86 | All |
| Operating System | Sun | Solaris | 8.0   | All | x86 | All |
| Operating System | Sun | Solaris | 2.4   | All | x86 | All |
| Operating System | Sun | Solaris | 2.5   | All | x86 | All |
| Operating System | Sun | Solaris | 2.5.1 | All | ppc | All |
| Operating System | Sun | Solaris | 2.5.1 | All | x86 | All |
| Operating System | Sun | Solaris | 2.6   | All | All | All |
| Operating System | Sun | Solaris | 7.0   | All | x86 | All |
| Operating System | Sun | Solaris | 8.0   | All | x86 | All |
| Operating System | Sun | Sunos   | -     | All | All | All |
| Operating System | Sun | Sunos   | 5.0   | All | All | All |
| Operating System | Sun | Sunos   | 5.1   | All | All | All |
| Operating System | Sun | Sunos   | 5.2   | All | All | All |
| Operating System | Sun | Sunos   | 5.3   | All | All | All |
| Operating System | Sun | Sunos   | 5.4   | All | All | All |
| Operating System | Sun | Sunos   | 5.5   | All | All | All |
| Operating System | Sun | Sunos   | 5.5.1 | All | All | All |
| Operating System | Sun | Sunos   | 5.7   | All | All | All |
| Operating System | Sun | Sunos   | 5.8   | All | All | All |
| Operating System | Sun | Sunos   | -     | All | All | All |
| Operating System | Sun | Sunos   | 5.0   | All | All | All |
| Operating System | Sun | Sunos   | 5.1   | All | All | All |
| Operating System | Sun | Sunos   | 5.2   | All | All | All |
| Operating System | Sun | Sunos   | 5.3   | All | All | All |
| Operating System | Sun | Sunos   | 5.4   | All | All | All |
| Operating System | Sun | Sunos   | 5.5   | All | All | All |
| Operating System | Sun | Sunos   | 5.5.1 | All | All | All |
| Operating System | Sun | Sunos   | 5.7   | All | All | All |
| Operating System | Sun | Sunos   | 5.8   | All | All | All |

| Reference                                                              | Source  | Link                                                                           | Tags                 |
|------------------------------------------------------------------------|---------|--------------------------------------------------------------------------------|----------------------|
| Search results                                                         | AIXAPAR | <a href="http://www-1.ibm.com">www-1.ibm.com</a>                               |                      |
| 20011212 Buffer Overflow in /bin/login                                 | ISS     | <a href="http://xforce.iss.net">xforce.iss.net</a>                             | Patch, Vendor Advi   |
| IBM X-Force Exchange                                                   | XF      | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |                      |
| Sun Security Bulletins Article 213                                     | SUN     | <a href="http://sunsolve.sun.com">sunsolve.sun.com</a>                         |                      |
| CSSA-2001-SCO.40                                                       | CALDERA | <a href="http://stage.caldera.com">stage.caldera.com</a>                       |                      |
| CERT Advisory CA-2001-34 Buffer Overflow in System V Derived Login     | CERT    | <a href="http://www.cert.org">www.cert.org</a>                                 | Patch, Third Party A |
| CERT/CC Vulnerability Note VU#569272                                   | CERT-VN | <a href="http://www.kb.cert.org">www.kb.cert.org</a>                           | US Government Re     |
| 20011201-01-I                                                          | SGI     | <a href="http://patches.sgi.com">patches.sgi.com</a>                           |                      |
| Repository / Oval Repository                                           | OVAL    | <a href="http://oval.cisecurity.org">oval.cisecurity.org</a>                   |                      |
| Multiple Vendor System V Derived 'login' Buffer Overflow Vulnerability | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               | Exploit, Patch, Venc |
| SecurityFocus HOME Mailing List: BugTraq                               | BUGTRAQ | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               | Vendor Advisory      |
| 20011214 Sun Solaris login bug patches out                             | BUGTRAQ | <a href="http://marc.info">marc.info</a>                                       |                      |
| CVE Program record                                                     | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                                   | canonical            |
| NVD vulnerability detail                                               | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                 | canonical, analysis  |

No vendor comments have been submitted for this CVE.

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