



# CVE-2002-1654

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

## Summary

<b>CVE</b>	CVE-2002-1654
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2002-12-31 05:00:00 UTC
<b>Updated</b>	2017-07-11 01:29:00 UTC
<b>Description</b>	iPlanet Web Server Enterprise Edition and Netscape Enterprise Server 4.0 and 4.1 allows remote attackers to conduct HTTP

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	6.0	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	enterprise_4.0	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	enterprise_4.1	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	6.0	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	enterprise_4.0	All	All	All
Application	<a href="#">Iplanet</a>	<a href="#">Iplanet Web Server</a>	enterprise_4.1	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	2.0	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.0	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.1	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.2	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.3	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.4	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.5	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.6	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	2.0	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.0	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.1	All	All	All

Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.2	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.3	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.4	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.5	All	All	All
Application	<a href="#">Netscape</a>	<a href="#">Enterprise Server</a>	3.6	All	All	All

## References

### Reference

SecurityTracker.com Archives - Netscape Enterprise Server Publishing Feature Allows Remote Users to Conduct Brute Force Password Guess

iPlanet Information for VU#985347

'Netscape Publishing wp-force-auth Command' - SecuriTeam

IBM X-Force Exchange

[VulnWatch] Netscape publishing wp-force-auth command

Procheckup.com Navigation Error

CERT/CC Vulnerability Note VU#985347

Netscape Enterprise Web Server Brute Force Authentication Attacks Vulnerability

CVE Program record

NVD vulnerability detail

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**