



CVE-2001-1452

Published on: 08/31/2001 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:18 PM UTC

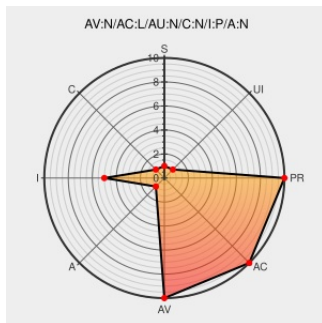
CVE-2001-1452

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Windows 2000](#) from [Microsoft](#) contain the following vulnerability:

By default, DNS servers on Windows NT 4.0 and Windows 2000 Server cache glue records received from non-delegated name servers, which allows remote attackers to poison the DNS cache via spoofed DNS responses.

CVE-2001-1452 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

How to prevent DNS cache pollution

[Vendor Advisory](#)
[support.microsoft.com](#)
[text/html](#)

[MSKB Q241352](#)

CERT/CC Vulnerability Note VU#109475

[Third Party Advisory](#)
[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#109475](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF nt-ms-dns-cachepollution\(3675\)](#)

Microsoft Windows DNS Resource Record Cache Corruption Vulnerability

[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 6791](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport website. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All

Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	All	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	All	server	All
Operating System	Microsoft	Windows Nt	4.0	All	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	server	All
Operating System	Microsoft	Windows Nt	4.0	sp1	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	server	All
Operating System	Microsoft	Windows Nt	4.0	sp2	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	server	All
Operating System	Microsoft	Windows Nt	4.0	sp3	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	server	All
Operating System	Microsoft	Windows Nt	4.0	sp4	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All

Operating System	Microsoft	Windows Nt	4.0	sp5	server	All
Operating System	Microsoft	Windows Nt	4.0	sp5	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	enterprise_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0*:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0*:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0*:terminal_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:terminal_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:terminal_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:enterprise_server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*:*:*:*:						
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:terminal_server:*:*:*:*:						

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:*:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:*:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:*:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp1:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp2:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp3:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp4:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp5:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:enterprise_server:*****:
cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023  |

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](#)