



CVE-2004-2131

Published on: 01/27/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2131

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Informix Dynamic Server](#) from [Ibm](#) contain the following vulnerability:

Stack-based buffer overflow in ontape for IBM Informix Dynamic Server (IDS) 9.40.xC3 and earlier allows local users, with DSA privileges, to execute arbitrary code via a long ONCONFIG environment variable.

CVE-2004-2131 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF informix-ontape-binary-bo\(14970\)](#)

IBM notice: The page you requested cannot be displayed

[Exploit](#)
[Patch](#)
[Vendor Advisory](#)
[www-1.ibm.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM www-1.ibm.com/support/docview.wss?uid=swg21153336](#)

Secunia - Advisories - IBM Informix Database Multiple Local Vulnerabilities

[web.archive.org](#)
[text/html](#)

[SECUNIA 10737](#)

'----- OPEN3S-2003-08-08-eng-informix-ontape' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040129 ----- OPEN3S-2003-08-08-eng-informix-ontape](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 3759](#)

Inactive Link Not Archived

IBM Informix Dynamic Server/Informix Extended Parallel Server Multiple Vulnerabilities

Exploit
Patch
Vendor Advisory
cve.report (archive)
text/html

BID 9512

By selecting these links, you may be leaving CVEreport webspace. 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
Application	ibm	Informix Dynamic Server	9.40.uc1	All	All	All
Application	ibm	Informix Dynamic Server	9.40.uc2	All	All	All
Application	ibm	Informix Dynamic Server	9.40.uc1	All	All	All
Application	ibm	Informix Dynamic Server	9.40.uc2	All	All	All
Application	ibm	Informix Extended Parallel Server	8.40_uc1	All	All	All
Application	ibm	Informix Extended Parallel Server	8.40_uc1	All	All	All

cpe:2.3:a:ibm:informix_dynamic_server:9.40.uc1:*:*:*:*:*:

cpe:2.3:a:ibm:informix_dynamic_server:9.40.uc2:*:*:*:*:*:

cpe:2.3:a:ibm:informix_dynamic_server:9.40.uc1:*:*:*:*:*:

cpe:2.3:a:ibm:informix_dynamic_server:9.40.uc2:*:*:*:*:*:

cpe:2.3:a:ibm:informix_extended_parallel_server:8.40_uc1:*:*:*:*:*:

cpe:2.3:a:ibm:informix_extended_parallel_server:8.40_uc1:*:*:*:*:*:

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](#).

