

IBM X-Force Exchange



X-Force Exchange

Dynamic Linker telnet gains root access

IBM X-Force Exchange is a threat intelligence sharing platform that you can use to research security threats, to aggregate intelligence, and to collaborate with peers.

CVE-1999-0073

Logged in users have integrated access to all the functionality of the site: searching, commenting, Collections and sharing. Guests can search and view reports only.

This report does not contain tags. Add tags via the comment box.

Report tags

I agree to the terms of this license ()
Related tags from configured third-party sources are also displayed here. [Create IBMid](#)

[Log In](#)

Details

The tags are either automatically inserted by XFE based on the author's report data or explicitly retrieved from the vendor's community.

linkerbug (67) **reported Oct 31, 1995**
You must log in () to use that feature

Many Telnet daemons offer the functionality of transferring environment variables from one system to another. On systems that run these daemons and also provide support for shared object libraries, a user could bypass typical authentication mechanisms in the login program by specifying an alternate location for the standard library. Depending on the system's configuration, either a local or remote attacker could gain root access on the affected system. The following environment variables are not typically passed, and could be used to bypass authentication mechanisms: - _RLD_LIST - _RLD_ROOT - ELF_LD_LIBRARY_PATH - LD_AOUT_LIBRARY_PATH - LIBPATH - LD_PRELOAD - LD_LIBRARY_PATH

Consequences:

Gain Access

Remedy

Determine if your telnet daemon uses the ENVIRON or NEW-ENVIRON options. If your daemon uses these options, your system may be vulnerable. Immediately disable the telnet daemon or apply the wrapper provided by CERT until you can obtain a patch from your vendor. See references.

If use of one of these environment variables has been detected, it should be considered suspicious, although it does not necessarily indicate an attack. Determine if this is in compliance with your system policies. Investigate whether this is part of normal usage, based on information including the source address, time, and frequency.

CVSS 1.0 Base Score

10

Access Vector	Remote
Access Complexity	Low
Authentication	Not Required
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete



Did you know that we have an X-Force Threat Intelligence API?

IBM® X-Force Exchange

X-Force threat intelligence is actionable and is available via our APIs (JSON and STIX), which can be ingested into SIEMs. — Read more at our [API documentation \(https://exchange.xforce.ibmcloud.com/api/doc/#Vulnerabilities_get_vulnerabilities_xfid\)](https://exchange.xforce.ibmcloud.com/api/doc/#Vulnerabilities_get_vulnerabilities_xfid)

IBM X-Force Exchange is a threat intelligence sharing platform that you can use to research security threats, to aggregate intelligence, and to collaborate with peers. Logged in users have integrated access to all the functionality of the site: searching, commenting, Collections and sharing. Guests can search and view reports only.

[Buy Now \(https://www.ibm.com/marketplace/purchase/configuration/en/us/checkout?editionID=EIDLI38T\)](https://www.ibm.com/marketplace/purchase/configuration/en/us/checkout?editionID=EIDLI38T)

I agree to the [Terms of Service \(\)](#)

IBM Network Protection

... or enter as a Guest ()

Coverage

Date

PAM [Telnet_Linkers_Bug](#)

Feb 21, 2005

Affected Products

Affected Products

Linux Kernel

NEC EWS-UX V

NEC UP-UX V

NEC ASL UX 4800

Dependent Products

Dependent Product

Compaq Tru64

Data General DG/UX

HP HP-UX

IBM AIX

References

External link

[CVE-1999-0073 \(https://www.cve.org/CVERecord?id=CVE-1999-0073\)](https://www.cve.org/CVERecord?id=CVE-1999-0073)

[CERT Advisory CA-1995-14 \(http://www.cert.org/advisories/CA-1995-14.html\)](http://www.cert.org/advisories/CA-1995-14.html)

External link

[SGI Security Advisory 19951101-01-P1010o1020](http://patches.sgi.com/support/free/security/advisories/19951101-01-P1010o1020)
(<http://patches.sgi.com/support/free/security/advisories/19951101-01-P1010o1020>)

IBM® X-Force Exchange

[IBM X-Force Exchange](http://www.ibm.com/xforce) is an intelligence sharing platform that you can use to research security threats, to aggregate intelligence, and to collaborate with peers.

Logged in users have integrated access to all the functionality of the site: searching, commenting, Collections and sharing. Guests can search and view reports only.

I agree to the Terms of Service (0) Comments (0) ()

Collections (0) / Reports (0) ()

Be the first person to comment.

... or enter as a Guest ()



Join the IBM X-Force Exchange Conversation.

[Log In](#)

Not a member? [Sign Up](#)



[API \(https://exchange.xforce.ibmcloud.com/api/doc/\)](https://exchange.xforce.ibmcloud.com/api/doc/)

[Support \(/faq#xforce_support\)](#)

[Provide Feedback \(\)](#)

[Make a Feature Request](#)

(https://www.ibm.com/developerworks/rfe/execute?use_case=changeRequestLanding&BRAND_ID=301&PROD_ID=1465)

[FAQ \(/faq\)](#)

[Service Status \(https://statuspage.ibm.com/\)](https://statuspage.ibm.com/)

[Privacy \(http://www.ibm.com/privacy\)](http://www.ibm.com/privacy)

[Terms \(\)](#)

[Invite \(mailto:?subject=Invitation%20to%20Join%20the%20IBM%20X-Force%20Exchange%20community&body=I%20would%20like%20to%20join%20the%20IBM%20X-Force%20Exchange%20community\)](mailto:?subject=Invitation%20to%20Join%20the%20IBM%20X-Force%20Exchange%20community&body=I%20would%20like%20to%20join%20the%20IBM%20X-Force%20Exchange%20community)

© 2014, 2026 IBM Security (<https://www.ibm.com/>)

Build 20260319