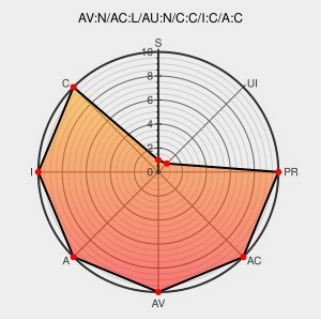
CVE-2004-0318

Published on: 03/18/2004 12:00:00 AM UTC

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

CVE-2004-0318

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Lsf from Platform contain the following vulnerability:

Load Sharing Facility (LSF) 4.x, 5.x, and 6.x uses the LSF_EAUTH_UID environment variable, if it exists, instead of the real UID of the user, which could allow remote attackers within the local cluster to gain privileges.

CVE-2004-0318 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
'Lam3rZ Security Advisory #2/2004: LSF eauth vulnerability leads to' - MARC	marc.info text/html	BUGTRAQ 20040223 Lam3rZ Security Advisory #2/2004: LSF eauth vulnerability leads to a possibility of controlling cluster jobs on behalf of other users
Platform Load Sharing Facility EAuth Privilege Escalation Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 9724
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF lsf-eauth-process-hijack(15278)

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	Platform	Lsf	4.0	All	All	All
Application	Platform	Lsf	4.2	All	All	All
Application	Platform	Lsf	5.0	All	All	All
Application	Platform	Lsf	5.1	All	All	All
Application	Platform	Lsf	6.0	All	All	All
Application	Platform	Lsf	4.0	All	All	All
Application	Platform	Lsf	4.2	All	All	All
Application	Platform	Lsf	5.0	All	All	All
Application	Platform	Lsf	5.1	All	All	All
Application	Platform	Lsf	6.0	All	All	All

cpe:2.3:a:platform:lsf:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:platform:lsf:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report