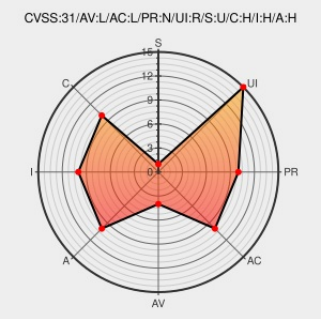
CVE-2019-19918

Published on: 12/20/2019 12:00:00 AM UTC

Last Modified on: 12/14/2022 06:36:00 PM UTC

CVE-2019-19918

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

Lout 3.40 has a heap-based buffer overflow in the srcnext() function in z02.c.

CVE-2019-19918 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:1772-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1772
[security-announce] openSUSE-SU-2020:1812-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1812

[SECURITY] Fedora 32 Update: lout-3.40-18.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-869cd99560
[SECURITY] Fedora 31 Update: lout-3.40-18.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-88fb82d1cd
Heap-based buffer overflow in the srcnext() function	Exploit Mailing List Third Party Advisory lists.gnu.org text/html	MISC lists.gnu.org/archive/html/lout-users/2019-12/msg00001.html
[security-announce] openSUSE-SU-2020:1771-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1771
[security-announce] openSUSE-SU-2020:1813-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1813
[SECURITY] Fedora 33 Update: lout-3.40-18.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-81c80ff1ed

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Lout Project	Lout	3.40	All	All	All
Application	Lout Project	Lout	3.40	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:a:lout_project:lout:3.40:*:*:*:*:*:*:*:

cpe:2.3:a:lout_project:lout:3.40:*:*:*:*:*:*:*

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*

cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*:*:*:*:*:*

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→