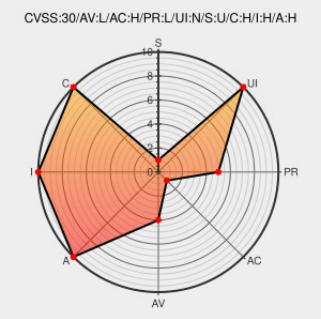
CVE-2018-3836

Published on: 04/24/2018 12:00:00 AM UTC

Last Modified on: 02/03/2023 06:48:00 PM UTC

CVE-2018-3836

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

An exploitable command injection vulnerability exists in the gplotMakeOutput function of Leptonica 1.74.4. A specially crafted gplot rootname argument can cause a command injection resulting in arbitrary code execution. An attacker can provide a malicious path as input to an application that passes attacker data to this function to trigger this vulnerability.

CVE-2018-3836 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Dan Bloomberg** - **Leptonica** version **1.74.4**

CVSS3 Score: 7.8 - HIGH

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

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

TALOS-2018-0516 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2018-0516
[SECURITY] [DLA 1284-1] leptonlib security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180215 [SECURITY] [DLA 1284-1] leptonlib security update

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Leptonica	Leptonica	1.74.4	All	All	All
Application	Leptonica	Leptonica	1.74.4	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:leptonica:leptonica:1.74.4:*:*:*:*:*:*:*:

cpe:2.3:a:leptonica:leptonica:1.74.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→