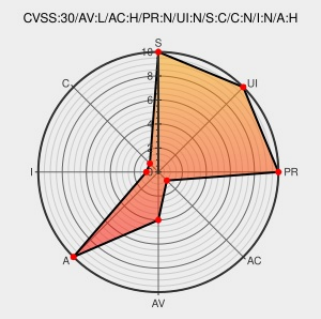
CVE-2019-5023

Published on: 10/31/2019 12:00:00 AM UTC

Last Modified on: 06/07/2022 06:41:00 PM UTC

CVE-2019-5023

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



Certain versions of Gresecurity from Gresecurity contain the following vulnerability:

An exploitable vulnerability exists in the grsecurity PaX patch for the function read_kmem, in PaX from version pax-linux-4.9.8-test1 to 4.9.24-test7, grsecurity official from version grsecurity-3.1-4.9.8-201702060653 to grsecurity-3.1-4.9.24-201704252333, grsecurity unofficial from version v4.9.25-unofficialgrsec to v4.9.74-unofficialgrsec. PaX adds a temp buffer to the read_kmem function, which is never freed when an invalid address is supplied. This results in a memory leakage that can lead to a crash of the system. An attacker needs to induce a read to /dev/kmem using an invalid address to exploit this vulnerability.

CVE-2019-5023 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
TALOS-2019-0784 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0784

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gresecurity	Gresecurity	All	All	All	All
Application	Gresecurity	Gresecurity	All	All	All	All
Application	Gresecurity	Pax	All	All	All	All
Application	Opensrcsec	Grsecurity	All	All	All	All
Application	Opensrcsec	Grsecurity	All	All	All	All
Application	Opensrcsec	Pax	All	All	All	All

cpe:2.3:a:gresecurity:gresecurity:*:*:*:*:official:*:*:*:

cpe:2.3:a:gresecurity:gresecurity:*:*:*:*:unofficial:*:*:*:

cpe:2.3:a:gresecurity:pax:*:*:*:*:*:*:*:*:

cpe:2.3:a:opensrcsec:grsecurity:*:*:*:*:official:*:*:*:

cpe:2.3:a:opensrcsec:grsecurity:*:*:*:*:unofficial:*:*:*:

cpe:2.3:a:opensrcsec:pax:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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.

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