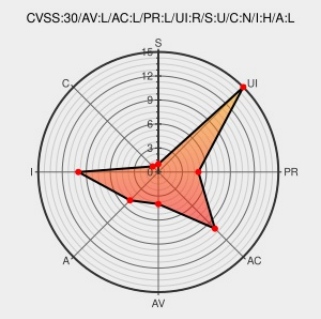
CVE-2018-6693

Published on: 09/18/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:00:00 AM UTC

CVE-2018-6693

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



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

An unprivileged user can delete arbitrary files on a Linux system running ENSLTP 10.5.1, 10.5.0, and 10.2.3 Hotfix 1246778 and earlier. By exploiting a time of check to time of use (TOCTOU) race condition during a specific scanning sequence, the unprivileged user is able to perform a privilege escalation to delete arbitrary files.

CVE-2018-6693 has been assigned by psirt@mcafee.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **McAfee** - **Endpoint Security for Linux Threat Prevention (ENSLTP)** version **10.5.0**

Affected Vendor/Software: **McAfee** - **Endpoint Security for Linux Threat Prevention (ENSLTP)** version **10.5.0**

Affected Vendor/Software: **McAfee** - **Endpoint Security for Linux Threat Prevention (ENSLTP)** version **10.2.3 Hotfix 1246778**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 3.3 - LOW

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

CVE References

Description	Tags	Link
McAfee Security Bulletin - Endpoint Security for Linux Threat Prevention update fixes privilege escalation vulnerability allowing unprivileged users to delete arbitrary files (CVE-2018-6693)	Vendor Advisory kc.mcafee.com text/html	CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10248

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Mcafee	Endpoint Security For Linux Threat Prevention	10.5.1	All	All	All
Application	Mcafee	Endpoint Security For Linux Threat Prevention	10.5.1	All	All	All
Application	Mcafee	Endpoint Security For Linux Threat Prevention	All	All	All	All
Application	Mcafee	Endpoint Security Linux Threat Prevention	10.5.0	All	All	All
Application	Mcafee	Endpoint Security Linux Threat Prevention	10.5.0	All	All	All

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:a:mcafee:endpoint_security_for_linux_threat_prevention:10.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:mcafee:endpoint_security_for_linux_threat_prevention:10.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:mcafee:endpoint_security_for_linux_threat_prevention:*:*:*:*:*:*:*:*:

cpe:2.3:a:mcafee:endpoint_security_linux_threat_prevention:10.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:mcafee:endpoint_security_linux_threat_prevention:10.5.0:*:*:*:*:*:*:*:

Discovery Credit

RACK911Labs.com

← Previous ID

Next ID→

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