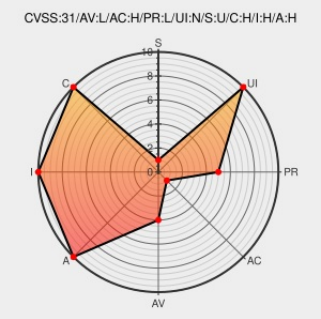
CVE-2021-23892

Published on: 05/12/2021 12:00:00 AM UTC

Last Modified on: 02/11/2023 06:36:00 PM UTC

CVE-2021-23892

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



Certain versions of Endpoint Security For Linux Threat Prevention from Mcafee contain the following vulnerability:

By exploiting a time of check to time of use (TOCTOU) race condition during the Endpoint Security for Linux Threat Prevention and Firewall (ENSL TP/FW) installation process, a local user can perform a privilege escalation attack to obtain administrator privileges for the purpose of executing arbitrary code through insecure use of predictable temporary file locations.

CVE-2021-23892 has been assigned by trellixpsirt@trellix.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **McAfee,LLC** - **McAfee Endpoint Security (ENS) for Linux** version **= unspecified**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link

McAfee Security Bulletin - Endpoint Security for Linux Threat Prevention and Firewall installer update fixes one vulnerability (CVE-2021-23892)	kc.mcafee.com text/html	CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10355

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mcafee	Endpoint Security For Linux Threat Prevention	All	All	All	All

cpe:2.3:o:mcafee:endpoint_security_for_linux_threat_prevention:*:*:*:*:*:linux:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23892 : By exploiting a time of check to time of use TOCTOU race condition during the Endpoint Security… twitter.com/i/web/status/1…	2021-05-12 09:16:00
/r/netcve	CVE-2021-23892	2021-05-12 09:41:40

← Previous ID

Next ID→