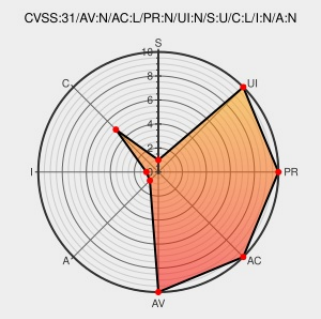
CVE-2020-10807

Published on: 03/22/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-10807

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



Certain versions of Caldera from Mitre contain the following vulnerability:

auth_svc in Caldera before 2.6.5 allows authentication bypass (for REST API requests) via a forged "localhost" string in the HTTP Host header.

CVE-2020-10807 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Patch0 by privateducky · Pull Request #1407 · mitre/caldera · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/mitre/caldera/pull/1407

Comparing 2.6.4...2.6.5 · mitre/caldera · GitHub	Third Party Advisory github.com text/html	MISC github.com/mitre/caldera/compare/2.6.4...2.6.5
Serious Security Flaw: API Requests from localhost · Issue #1405 · mitre/caldera · GitHub	Third Party Advisory github.com text/html	MISC github.com/mitre/caldera/issues/1405
Release 2.6.5 · mitre/caldera · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/mitre/caldera/releases/tag/2.6.5

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mitre	Caldera	All	All	All	All
Application	Mitre	Caldera	All	All	All	All

cpe:2.3:a:mitre:caldera:*:*:*:*:*:*:*:*:

cpe:2.3:a:mitre:caldera:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→