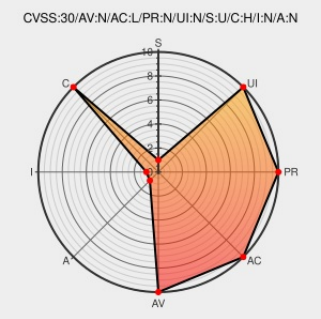
CVE-2018-6460

Published on: 01/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:48 PM UTC

CVE-2018-6460

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



Certain versions of Hotspot Shield from Anchorfree contain the following vulnerability:

Hotspot Shield runs a webserver with a static IP address 127.0.0.1 and port 895. The web server uses JSONP and hosts sensitive information including configuration. User controlled input is not sufficiently filtered: an unauthenticated attacker can send a POST request to /status.js with the parameter func=$_APPLOG.Rfunc and extract sensitive information about the machine, including whether the user is connected to a VPN, to which VPN he/she is connected, and what is their real IP address.

CVE-2018-6460 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	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
Hotspot Shield - Information Disclosure - Windows local	Exploit	EXPLOIT-DB 44042

Hotspot Shield - Information Disclosure - Windows local Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 44042
401 Authorization Required	Exploit Third Party Advisory blogs.securiteam.com text/html Inactive Link Not Archived	MISC blogs.securiteam.com/index.php/archives/3604

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
Application	Anchorfree	Hotspot Shield	-	All	All	All
Application	Anchorfree	Hotspot Shield	-	All	All	All

cpe:2.3:a:anchorfree:hotspot_shield:-:*:*:*:*:*:*:*:

cpe:2.3:a:anchorfree:hotspot_shield:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→