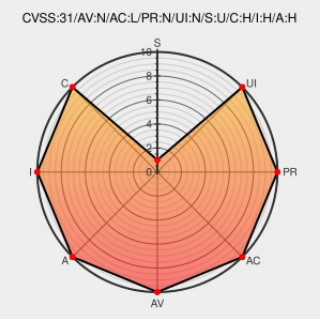
CVE-2020-13167

Published on: 05/19/2020 12:00:00 AM UTC

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

CVE-2020-13167

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



Certain versions of Netsweeper from Netsweeper contain the following vulnerability:

Netsweeper through 6.4.3 allows unauthenticated remote code execution because webadmin/tools/unixlogin.php (with certain Referer headers) launches a command line with client-supplied parameters, and allows injection of shell metacharacters.

CVE-2020-13167 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
SSD Advisory - Netsweeper PreAuth RCE - SSD Secure Disclosure	Exploit Third Party Advisory ssd-disclosure.com text/html	MISC ssd-disclosure.com/ssd-advisory-netsweeper-preauth-rce/

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	Netsweeper	Netsweeper	All	All	All	All

cpe:2.3:a:netsweeper:netsweeper:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@wvuuuuuuuuuuuu	Reminds me of Netsweeper CVE-2020-13167. Also entirely different from the command injection in /storfs-asup. Yikes. twitter.com/thezdi/status/…	2021-06-24 04:22:48
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-13167. … twitter.com/i/web/status/1…	2022-04-29 14:02:01
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-13167. #S7owtptljngd2y	2022-04-29 14:02:02

← Previous ID

Next ID→