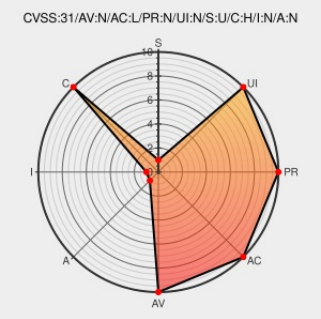
CVE-2019-13063

Published on: 09/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-13063

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



Certain versions of Sahi Pro from Sahipro contain the following vulnerability:

Within Sahi Pro 8.0.0, an attacker can send a specially crafted URL to include any victim files on the system via the script parameter on the Script_view page. This will result in file disclosure (i.e., being able to pull any file from the remote victim application). This can be used to steal and obtain sensitive config and other files. This can result in complete compromise of the application. The script parameter is vulnerable to directory traversal and both local and remote file inclusion.

CVE-2019-13063 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
Sahi pro 8.x - Directory Traversal - Multiple webapps Exploit	Exploit	EXPLOIT-DB Exploit Database

Sahi pro 8.x - Directory Traversal - Multiple Webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB Exploit Database
Download Archive | Sahi	Vendor Advisory sahipro.com text/html	MISC sahipro.com/downloads-archive/

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

Exploit/POC from Github

Proof of concept tool to exploit the directory traversal and local file inclusion vulnerability that resides in the S…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sahipro	Sahi Pro	8.0.0	All	All	All
Application	Sahipro	Sahi Pro	8.0.0	All	All	All

cpe:2.3:a:sahipro:sahi_pro:8.0.0:*:*:*:*:*:*:*

cpe:2.3:a:sahipro:sahi_pro:8.0.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→