



CVE-2020-14947

Published on: 06/30/2020 12:00:00 AM UTC

Last Modified on: 01/28/2023 02:38:00 AM UTC

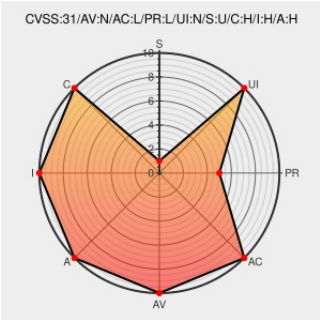
CVE-2020-14947

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Open Computer Software Inventory Next Generation](#) from [Factorfx](#) contain the following vulnerability:

OCS Inventory NG 2.7 allows Remote Command Execution via shell metacharacters to require/commandLine/CommandLine.php because mib_file in plugins/main_sections/ms_config/ms_snmp_config.php is mishandled in get_mib_oid.

CVE-2020-14947 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
OCS Inventory NG 2.7 Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158293/OCS-Inventory-NG-2.7-Remote-Code-Execution.html

Fix CVE-2020-14947 · OCSInventory-NG/OCSInventory-ocsreports@da72e0f · GitHub

github.com
text/html

CONFIRM github.com/OCSInventory-NG/OCSInventory-ocsreports/commit/da72e0fddaee44fbbd7241e07e5d53d1eee64

OCS.mp4 - Google Drive

Exploit
Third Party Advisory
web.archive.org
text/html
Inactive Link Not Archived

MISC drive.google.com/file/d/1-LVfL5ui5m2QfQxr0fDopzSECd4fTNRQ/view?usp=sharing

OCS Inventory NG v2.7 Remote Command Execution (CVE-2020-14947) - Shells.Systems

Exploit
Third Party Advisory
shells.systems
text/html

MISC shells.systems/ocs-inventory-ng-v2-7-remote-command-execution-cve-2020-14947/

OCSNG.py · GitHub

Exploit
Third Party Advisory
gist.github.com
text/html

MISC gist.github.com/mhaskar/233436d3096d4a7beafe36ff61dc2c73

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

The official exploit for OCS Inventory NG v2.7 Remote Command Execution CVE-2020-14947

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Factorfx	Open Computer Software Inventory Next Generation	2.7	All	All	All
Application	Factorfx	Open Computer Software Inventory Next Generation	2.7	All	All	All

cpe:2.3:a:factorfx:open_computer_software_inventory_next_generation:2.7:*:*:*:*:*:

cpe:2.3:a:factorfx:open_computer_software_inventory_next_generation:2.7:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Attackerkb_Bot	A new #attackerkb assesment on 'CVE-2020-14947' has been created by noraj. Attacker Value: 5 Exploitability: 5 attackerkb.com/assessments/c5...	2021-09-28 22:49:07
@ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2020-14947... twitter.com/i/web/status/1...	2022-03-31 10:02:01
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-14947. ipssignatures.appspot.com/?cve=CVE-2020-... #Sml5ndclixpwm	2022-03-31 10:02:01

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)