



# CVE-2022-42972

Published on: Not Yet Published

Last Modified on: 02/08/2023 07:40:00 PM UTC

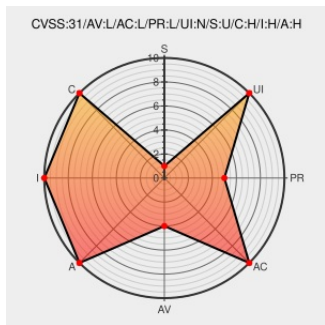
## CVE-2022-42972

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Windows 10** from **Microsoft** contain the following vulnerability:

A CWE-732: Incorrect Permission Assignment for Critical Resource vulnerability exists that could cause local privilege escalation when a local attacker modifies the webroot directory. Affected Products: APC Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GA), APC Easy UPS

Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GA-01-22261), Schneider Electric Easy UPS Online Monitoring Software (Windows 7, 10, 11 & Windows Server 2016, 2019, 2022 - Versions prior to V2.5-GS), Schneider Electric Easy UPS Online Monitoring Software (Windows 11, Windows Server 2019, 2022 - Versions prior to V2.5-GS-01-22261)

CVE-2022-42972 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Schneider Electric - APC Easy UPS Online Monitoring Software** version < **V2.5-GA**

Affected Vendor/Software: **Schneider Electric - APC Easy UPS Online Monitoring Software** version < **V2.5-GA-01-22261**


Affected Vendor/Software: **Schneider Electric - Schneider Electric Easy UPS Online Monitoring Software** version < **V2.5-GS**

Affected Vendor/Software: **Schneider Electric - Schneider Electric Easy UPS Online Monitoring Software** version < **V2.5-GS-01-22261**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References

Description	Tags	Link
No Description Provided	<a href="https://download.schneider-electric.com">download.schneider-electric.com</a> Inactive Link Not Archived	 MISC <a href="https://download.schneider-electric.com/files?p_Doc_SEVD-2022-347-01&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2022-347-01_Easy_UPS_Online_Monitoring_Software_Security_Notification.pdf">download.schneider-electric.com/files?p_Doc_SEVD-2022-347-01&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2022-347-01_Easy_UPS_Online_Monitoring_Software_Security_Notification.pdf</a>

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](mailto:comment@cve.report).

## Related QID Numbers

591411 Schneider Electric APC Easy UPS Online Monitoring Software Multiple Vulnerabilities (SEVD-2022-347-01 V2.0)

## Exploit/POC from Github

A CWE-732: Incorrect Permission Assignment for Critical Resource vulnerability exists that could cause local privileg...

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 11	-	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2022	-	All	All	All
Application	Schneider-electric	Apc Easy Ups Online Monitoring Software	All	All	All	All
Application	Schneider-electric	Easy Ups Online Monitoring Software	All	All	All	All

cpe:2.3:o:microsoft:windows\_10:-:\*:\*:\*:\*:\*:

cpe:2.3:o:microsoft:windows\_11:-:\*:\*:\*:\*:\*:

cpe:2.3:o:microsoft:windows\_7:-:\*:\*:\*:\*:\*:

cpe:2.3:o:microsoft:windows\_server\_2016:-:\*:\*:\*:\*:\*:

cpe:2.3:o:microsoft:windows\_server\_2019:-:\*:\*:\*:\*:\*:


cpe:2.3:o:microsoft:windows\_server\_2022:-:\*:\*:\*:\*:\*:

cpe:2.3:a:schneider-electric:apc\_easy\_ups\_online\_monitoring\_software:\*:\*:\*:\*:\*:\*:

cpe:2.3:a:schneider-electric:easy\_ups\_online\_monitoring\_software:\*:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	<a href="#">CVE-2022-42972</a>	2023-02-01 04:38:43

[← Previous ID](#)

[Next ID →](#)

© [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](#)