



CVE-2020-6140

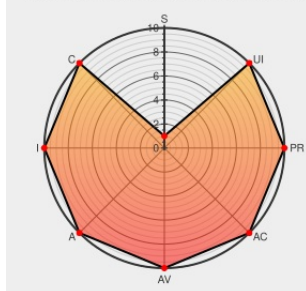
Published on: 09/01/2020 12:00:00 AM UTC

Last Modified on: 05/31/2022 07:49:00 PM UTC

CVE-2020-6140

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Opensis](#) from [Os4ed](#) contain the following vulnerability:

SQL injection vulnerability exists in the password reset functionality of OS4Ed openSIS 7.3. The password_stf_email parameter in the password reset page /opensis/ResetUserInfo.php is vulnerable to SQL injection. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2020-6140 has been assigned by [Cisco Talos](#) talos-cna@cisco.com 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

TALOS-2020-1080 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

[Exploit](#)

[Third Party Advisory](#)

[talosintelligence.com](#)

[MISC](#)

talosintelligence.com/vulnerability_reports/TALOS-2020-1080

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	Os4ed	Opensis	7.3	All	All	All
Application	Os4ed	Opensis	7.3	All	All	All
cpe:2.3:a:os4ed:opensis:7.3:*:*:*:-:*:*:						
cpe:2.3:a:os4ed:opensis:7.3:*:*:*:-:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ??? SQL injection vulnerability exists in th... CVE-2020-6140 Link for more: alerts.remotelyrmm.com/CVE-2020-6140	2022-04-28 20:34:10
 @LinInfoSec	Php - CVE-2020-6140: talosintelligence.com/vulnerability_...	2022-05-31 21:00:27

[← 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