Security advisory

Multiple Stored Cross Site Scripting (IrisNext 9.5.16)

June, 2021

CVE-2021-27930
Release date: 29/06/2021
Department: POST Cyberforce
Khalid ESSALMI

Vulnerability summary

Product	IrisNext
Product homepage	https://iriscorporate.com
Affected product versions	9.5.16
Severity	Medium: CVSS v3.1 score 5.4
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
MITRE ATT&CK	T1059, TA0002
OWASP	OWASP 2017-A7
CWE	CWE-79
Workarounds	No workarounds available
Fixed product versions	9.5.18 and later

Validated impact:

- Client-side remote code execution;
- Users sessions hi-jacking;
- Privilege escalation;

Timeline

Date	Action
February 23th, 2021	Vulnerability identification during pentest mission.
March 2nd, 2021	First contact with the editor (IrisNext Team).
March 3rd, 2021	Submit a CVE request to https://cveform.mitre.org/
March 3rd, 2021	Ticket created for CVE ID Request ”1037953”.
March 3rd, 2021	CVE-2021-27930 attributed by Mitre.
March 4th, 2021	2nd contact with the editor to inform him that CVE-2021-27930 was attributed.
March 4th, 2021	3rd contact with another platform ”Conversation ID: 157590” -> https://support.irislink.com/en-us/conversation/new/2
March 8th, 2021	1st response from IrisNext Team. Advisory sent to IRISNext R&D product manager.
March 11th, 2021	Fix release in IrisNext Edition 9.5.17
March 23th, 2021	Test of IrisNext Edition 9.5.17 -> The fix is not efficient.
March 25th, 2021	Fix release in IrisNext Edition 9.5.18.
March 25th, 2021	Test of IrisNext Edition 9.5.18 -> Fixed.
June 16th, 2021	Inform IrisNext that the Advisory will be published by the end of June.

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27930
- https://attack.mitre.org/techniques/T1059/
- https://attack.mitre.org/tactics/TA0002/
- https://owasp.org/www-project-top-ten/2017/de/A7_2017-Cross-Site_Scripting_(XSS)
- https://cwe.mitre.org/data/definitions/79.html

Product description

IRISNext is an electronic content management, allows document management and business process Mmanagement, directly within the browser:
1- Document management:

- dematerialized, indexed, centralized and traceable content;
- document retrieval;
- collaborative work (document edition, MS Office integration).

2- Business process management:

- tasks (distribution, schedules, sequencing and follow-up);
- customizable business workflows (ex. invoice approval, including line items, routing of requests, etc.).

Advisory

During the penetration test POST Cyberforce identified multiple stored XSS vulnerabilities in IrisNext Edition 9.5.16, which allows an authenticated (or compromised) user to inject malicious Javascript in folder/file name within the application in order to grab other users' sessions or execute malicious code in their browsers (1-click RCE).

Vulnerability description

The application allows users to edit and share docuements/folders. However, by injection a malicious Javascript in documents/folders names it's possible to redirect users to malicious website, grab their sessions or execute malicious code in their browsers.

Once an authenticated user try to delete document/folder (in which the JS script was injected), the code will be automatically executed. It is important to mention that this attack is possible from all users who have edit feature.

Proof of concept

Here are the steps to reproduce:
1) Login on the IrisNext application;
2) Go to 'Document tree';

3) Create a new folder with JS inside (from security option, check if this folder is shared, otherwise share it with other users);
4) From another user session, browser this folder –> click on it and try to delete it –> JS code will automatically executed.

Recommendation

- Upgrade to IrisNext Edition 9.5.18 or later.