kx90 Multiple Stored XSS (IrisNext 9.5.16) ... History

1 contributor

121 KB

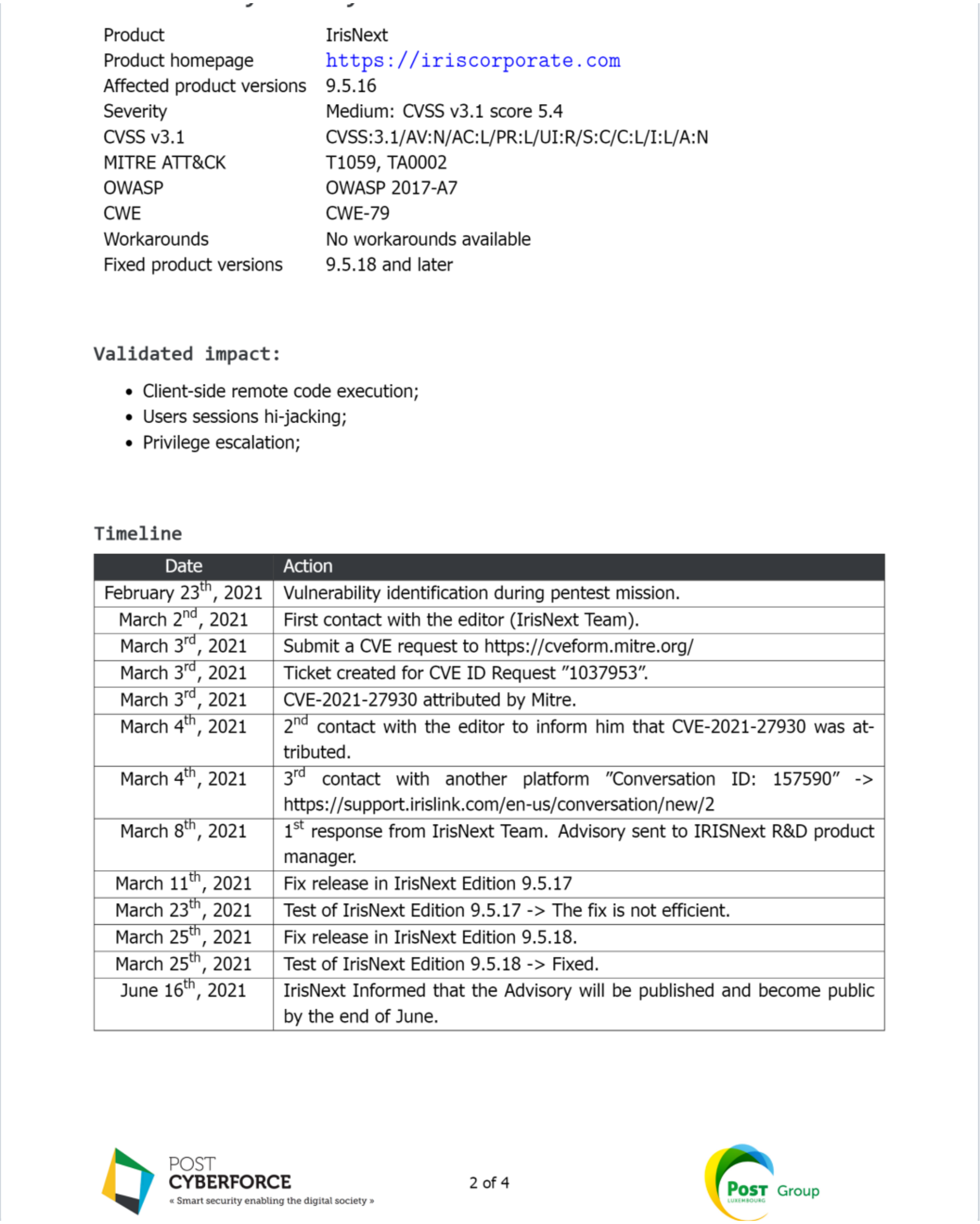
Security advisory

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	IrisNext Informed that the Advisory will be published and become public by the end of June.