darksh3llRU DSKNet advisory public release ... History

1 contributor

653 KB

Security advisory

Multiple vulnerabilities in the DSKNet Intranet web application

Affected versions before 2.20.137.1

July, 2022

CVE-2022-24688
CVE-2022-24689
CVE-2022-24690
CVE-2022-24691
CVE-2022-24692
Release date: 15/07/2022
Department: POST Cyberforce
Roman Zakharov

Vulnerabilities summary

Product	DSKNet Intranet web application
Product homepage	https://dsk.lu/fr/produits/temps-de-presence
Affected product versions	before 2.20.137.0
MITRE ATT&CK	T1190, T1078, T1110, T1189, T1185, T1059, T1505.003
Workaround	Partially provided
Fixed product versions	2.20.137.1

Vulnerability	Broken access control
CVE ID	CVE-2022-24689
Severity	High: CVSS v3.1 base score - 7.5
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
OWASP	OWASP 2021-A1
CWE	CWE-732

Vulnerability	Unauthenticated SQL injection
CVE ID	CVE-2022-24690
Severity	Critical: CVSS v3.1 base score - 9.3
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-89

Vulnerability	Multiple authenticated SQL injection
CVE ID	CVE-2022-24691
Severity	High: CVSS v3.1 base score - 8.5
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-89

Vulnerability	Stored Cross-site scripting
CVE ID	CVE-2022-24692
Severity	Medium: CVSS v3.1 base score - 6.9
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N
OWASP	OWASP 2021-A3
CWE	CWE-79

Vulnerability	Arbitrary file upload
CVE ID	CVE-2022-24688
Severity	High: CVSS v3.1 base score - 7.2
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
OWASP	OWASP 2021-A5
CWE	CWE-434

Exploitation impact:

- Unauthorized access
- Sensitive information disclosure
- Admin/User accounts takeover
- Remote code execution

Timeline

Date	Action
04 February 2022	Vulnerabilities identification, exploitation, and impact validation
07 February 2022	The vendor was notified and advised on mitigation actions
08 February 2022	The vendor acknowledged the vulnerabilities
09 February 2022	CVE-2022-24688 -> CVE-2022-24692 were assigned by MITRE
09 February 2022	The vendor was informed about assigned CVE IDs
09 February 2022	CIRCL was informed about assigned CVE IDs
09 February 2022	POST CSIRT was team informed about assigned CVE IDs
18 February 2022	Received an update from vendor, the COS team tested the updated version, not all vulnerabilities are fixed
11 March 2022	The vendor published a new release 2.20.137.1 addressing the issues
15 July 2022	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24688
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24689
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24690
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24691
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24692
- https://github.com/post-cyberlabs/CVE-Advisory/blob/main/CVE-2022-24688-92.pdf
- https://attack.mitre.org/techniques/T1190/
- https://attack.mitre.org/techniques/T1078/
- https://attack.mitre.org/techniques/T1110/
- https://attack.mitre.org/techniques/T1189/
- https://attack.mitre.org/techniques/T1185/
- https://attack.mitre.org/techniques/T1059/
- https://attack.mitre.org/techniques/T1505/003/
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://owasp.org/Top10/A03_2021-Injection/
- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://cwe.mitre.org/data/definitions/79.html
- https://cwe.mitre.org/data/definitions/89.html
- https://cwe.mitre.org/data/definitions/732.html
- https://cwe.mitre.org/data/definitions/434.html

Product description

The DSKNet intranet application allows the employees to access their presence data:

- DSKNet offers interactive access to employee's presence time data from any extension connected to your network. Use is possible internally and from outside, on any computer or mobile. The interface is compatible with the main browsers including Internet Explorer, Firefox, Safari, or Google Chrome.
- Modular architecture allows selecting the features to be used.

More information can be found by visiting the product webpage:
https://dsk.lu/fr/produits/temps-de-presence.

Advisory

Several security vulnerabilities were discovered in the DSKNet web application that can be chained to achieve the Remote Code Execution as the webserver user. The affected application versions are before 2.20.137.1.

The broken access control allows unauthenticated attackers to access the application's endpoints that disclose information about users' full names, badge numbers, departments, emails, and including their personal data such as Luxembourgish "matricule". The attacker can get unauthorized access to the application by brute-forcing the badge PIN code. Some user accounts have the "default" PIN code configured that simplifies the brute-force attack.

Multiple endpoints are vulnerable to the blind SQL injection attack that can be executed by unauthenticated and authenticated users. This attack simplifies the process to get the highest privileges within the application in order to proceed with the next vulnerability exploitation.

Discovered Stored Cross-site Scripting (XSS) permits delivering the end-user malicious code, stealing their cookies, and/or keeping access to the application after the user's PIN code changes. This XSS attack was abused to deliver malicious code and achieve client-side code execution. The exploitation requires user privileges with access to a specific configuration page.

To achieve Remote Code Execution the attacker requires to hijack a user with access to the specific configuration page. There are at least 3 ways to achieve that:

- Abuse broken access control to discover the user's badge number and conduct a brute-force attack to find the user with desired access.
- Abuse broken access control and conduct SQL injection attack that does not require authentication.
- Abuse regular user access and conduct authenticated SQL injection attack to discover badge number and PIN code for the user with access to the specific page.

To achieve Remote Code Execution the attacker abuses the specific menu configuration by uploading the malicious file (mimicking PDF) and enabling displaying the PDF for touch devices. By visiting the URL for the "Touch" devices the uploaded file is placed in the special web folder resulting in Remote Code Execution on the webserver.

Possible attacks schema

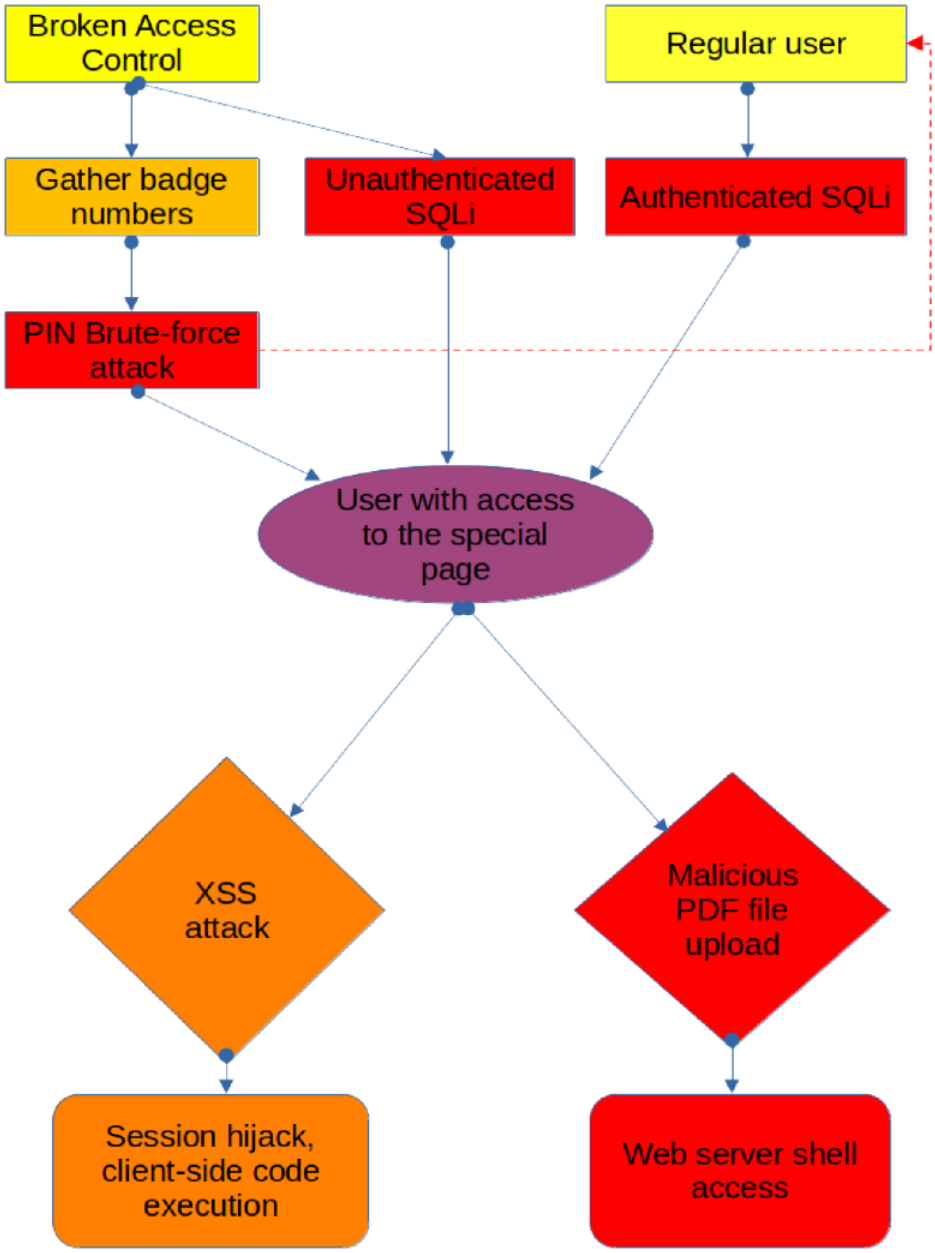

Figure 1: Attacks schema abusing discovered vulnerabilities

More Pages