microsoft / **XmlNotepad** Public

Code | Issues 47 | Pull requests 2 | Actions | Projects | Models | Wik

Commit 3665603

lovettchris committed last week · ✓ 5 / 5

```
Add user prompt on Ignore DTD setting changes that point to documentation
describing the risks.
```

master · 2.9.0.21

1 parent c03ab23 commit 3665603

7 files changed +128 -29 lines changed

Top

Filter files…

- docs/help
  - validation.md
- src
  - Application
    - Application.csproj
    - FormOptions.cs
  - Model
    - Settings.cs
  - Updates
    - Updates.xml
  - Version
    - Version.props
  - XmlNotepadSetup
    - Product.wxs

7 files changed +128 -29 lines changed

Search within code

docs/help/validation.md

```
@@ -13,8 +13,7 @@ and attribute names and values.
13 13
14 14  ## DTD Entity Leakage
15 15
16    - Users must be careful about which DTD's they allow XML Notepad to process.
      There is a well known attack using malicious DTD's that works like this.  A
      safer example of this is included
17    - in the XML Notepad samples folder named `DtdEntityLeakage.xml`:
   16 + Users must be careful about which DTD's they allow XML Notepad to process.
      There is a well known attack using malicious DTD's that works like this:
18 17
19 18
20 19  **Step 1** - Create `bait.xml`:
@@ -28,7 +27,7 @@ in the XML Notepad samples folder named
28 27
29 28  **Step 2** - User open `bait.xml` in XML Notepad, unaware that is a malicious
      XML file.
30 29
31    - **Result:** XML Notepad immediately makes an outbound HTTP GET request to the
      listener```
   30 + **Result:** XML Notepad immediately makes an outbound HTTP GET request to the
      listener
32 31
33 32  **The malicious DTD contains parameter entities that read local secrets**
34 33  and then sends those secrets to someplace as URL query parameters:
@@ -38,6 +37,8 @@ parameters:
38 37  <!ENTITY bad "<![CDATA[%leak;]]>">
39 38  ```
40 39
   40 + A safe example of this is included in the XML Notepad samples folder named
      `DtdEntityLeakage.xml`.
   41 +
41 42  ### Impact
42 43
```

```
43  44    Any user who opens a specially crafted XML file in XML Notepad is vulnerable —
          no clicks beyond opening the file are required. An attacker can use this capture
          secrets from your
          @@ -54,7 +55,7 @@ and set `Ignore DTD=False` under Validation options.
54  55    A malicious DTD can also contain entities that explode into gigabytes of memory
          by writing
55  56    something like this:
56  57
57      - ```
    58  + ```xml
58  59    <!ENTITY e0 "This is some long text that we will replicate exponentially">
59  60    <!ENTITY e1 "&e0;&e0;&e0;&e0;&e0;&e0;&e0;&e0;&e0;&e0;">
60  61    <!ENTITY e2 "&e1;&e1;&e1;&e1;&e1;&e1;&e1;&e1;&e1;&e1;">
```

src/Application/Application.csproj

```
          @@ -34,6 +34,8 @@
34  34        <PublisherName>Chris Lovett</PublisherName>
35  35        <WebPage>readme.htm</WebPage>
36  36        <DisallowUrlActivation>true</DisallowUrlActivation>
    37  +     <ApplicationRevision>20</ApplicationRevision>
    38  +     <ApplicationVersion>2.9.0.20</ApplicationVersion>
37  39        <UseApplicationTrust>false</UseApplicationTrust>
38  40        <PublishWizardCompleted>true</PublishWizardCompleted>
39  41        <BootstrapperEnabled>true</BootstrapperEnabled>
          @@ -171,7 +173,8 @@
171 173       <Compile Include="FormSearch.Designer.cs">
172 174         <DependentUpon>FormSearch.cs</DependentUpon>
173 175       </Compile>
174     -     <Compile Include="Program.cs"></Compile>
    176 +     <Compile Include="Program.cs">
    177 +     </Compile>
175 178       <Compile Include="Properties\AssemblyInfo.cs" />
176 179       <Compile Include="Win32Helpers.cs" />
177 180       <Compile Include="XmlDiffWrapper.cs" />
          @@ -254,6 +257,10 @@
254 257         <CopyToOutputDirectory>PreserveNewest</CopyToOutputDirectory>
255 258         <Generator>SettingsSingleFileGenerator</Generator>
```

```
256 259         </Content>
    260 +     <Content Include="Samples\DtdEntityExplosion.xml">
    261 +       <SubType>Designer</SubType>
    262 +       <CopyToOutputDirectory>PreserveNewest</CopyToOutputDirectory>
    263 +     </Content>
257 264         <Content Include="Samples\DtdEntityLeakage.xml">
258 265           <SubType>Designer</SubType>
259 266           <CopyToOutputDirectory>PreserveNewest</CopyToOutputDirectory>
        @@ -311,64 +318,110 @@
311 318       <ItemGroup>
312 319         <PublishFile Include="Samples\basket.xml">
313 320           <Visible>False</Visible>
314     -       <Group></Group>
315     -       <TargetPath></TargetPath>
    321 +       <Group>
    322 +       </Group>
    323 +       <TargetPath>
    324 +       </TargetPath>
316 325           <PublishState>Include</PublishState>
317 326           <IncludeHash>True</IncludeHash>
318 327           <FileType>File</FileType>
319 328         </PublishFile>
320 329         <PublishFile Include="Samples\basket.xsd">
321 330           <Visible>False</Visible>
322     -       <Group></Group>
323     -       <TargetPath></TargetPath>
    331 +       <Group>
    332 +       </Group>
    333 +       <TargetPath>
    334 +       </TargetPath>
    335 +       <PublishState>Include</PublishState>
    336 +       <IncludeHash>True</IncludeHash>
    337 +       <FileType>File</FileType>
    338 +     </PublishFile>
    339 +     <PublishFile Include="Samples\DtdEntityExplosion.xml">
    340 +       <Visible>False</Visible>
    341 +       <Group>
    342 +       </Group>
    343 +       <TargetPath>
```

```
      344 +        </TargetPath>
      345 +        <PublishState>Include</PublishState>
      346 +        <IncludeHash>True</IncludeHash>
      347 +        <FileType>File</FileType>
      348 +      </PublishFile>
      349 +      <PublishFile Include="Samples\DtdEntityLeakage.xml">
      350 +        <Visible>False</Visible>
      351 +        <Group>
      352 +        </Group>
      353 +        <TargetPath>
      354 +        </TargetPath>
 324  355          <PublishState>Include</PublishState>
 325  356          <IncludeHash>True</IncludeHash>
 326  357          <FileType>File</FileType>
 327  358        </PublishFile>
 328  359        <PublishFile Include="Samples\Employee.xml">
 329  360          <Visible>False</Visible>
 330      -        <Group></Group>
 331      -        <TargetPath></TargetPath>
      361 +        <Group>
      362 +        </Group>
      363 +        <TargetPath>
      364 +        </TargetPath>
 332  365          <PublishState>Include</PublishState>
 333  366          <IncludeHash>True</IncludeHash>
 334  367          <FileType>File</FileType>
 335  368        </PublishFile>
 336  369        <PublishFile Include="Samples\Employee.xsd">
 337  370          <Visible>False</Visible>
 338      -        <Group></Group>
 339      -        <TargetPath></TargetPath>
      371 +        <Group>
      372 +        </Group>
      373 +        <TargetPath>
      374 +        </TargetPath>
 340  375          <PublishState>Include</PublishState>
 341  376          <IncludeHash>True</IncludeHash>
 342  377          <FileType>File</FileType>
 343  378        </PublishFile>
 344  379        <PublishFile Include="Samples\Hamlet.xml">
```

```
345  380          <Visible>False</Visible>
346       -       <Group></Group>
347       -       <TargetPath></TargetPath>
     381  +       <Group>
     382  +       </Group>
     383  +       <TargetPath>
     384  +       </TargetPath>
     385  +       <PublishState>Include</PublishState>
     386  +       <IncludeHash>True</IncludeHash>
     387  +       <FileType>File</FileType>
     388  +     </PublishFile>
     389  +     <PublishFile Include="Samples\MaliciousDtd.dtd">
     390  +       <Visible>False</Visible>
     391  +       <Group>
     392  +       </Group>
     393  +       <TargetPath>
     394  +       </TargetPath>
348  395          <PublishState>Include</PublishState>
349  396          <IncludeHash>True</IncludeHash>
350  397          <FileType>File</FileType>
351  398        </PublishFile>
352  399        <PublishFile Include="Samples\rss.xml">
353  400          <Visible>False</Visible>
354       -       <Group></Group>
355       -       <TargetPath></TargetPath>
     401  +       <Group>
     402  +       </Group>
     403  +       <TargetPath>
     404  +       </TargetPath>
356  405          <PublishState>Include</PublishState>
357  406          <IncludeHash>True</IncludeHash>
358  407          <FileType>File</FileType>
359  408        </PublishFile>
360  409        <PublishFile Include="Samples\rsspretty.xsl">
361  410          <Visible>False</Visible>
362       -       <Group></Group>
363       -       <TargetPath></TargetPath>
     411  +       <Group>
     412  +       </Group>
     413  +       <TargetPath>
```

```
                414 +       </TargetPath>
364             415         <PublishState>Include</PublishState>
365             416         <IncludeHash>True</IncludeHash>
366             417         <FileType>File</FileType>
367             418       </PublishFile>
368             419       <PublishFile Include="Samples\willy.xsl">
369             420         <Visible>False</Visible>
370             -       <Group></Group>
371             -       <TargetPath></TargetPath>
                421 +       <Group>
                422 +       </Group>
                423 +       <TargetPath>
                424 +       </TargetPath>
372             425         <PublishState>Include</PublishState>
373             426         <IncludeHash>True</IncludeHash>
374             427         <FileType>File</FileType>
```

src/Application/FormOptions.cs

```
                    @@ -1,4 +1,4 @@
1                   - using System;
                  1 + using System;
2                 2   using System.Drawing;
3                 3   using System.Collections;
4                 4   using System.ComponentModel;
                    @@ -102,6 +102,7 @@ public override ISite Site
102             102                     {
103             103                         this._settings = value.GetService(typeof(Settings)) as
                    Settings;
104             104                         this._userSettings = new UserSettings(this._settings) {
                    Font = this.SelectedFont };
                  105 +                   this._userSettings.EnableDtdHandler += HandleEnableDtd;
105             106
106             107                         List<string> hiddenProperties = new List<string>();
107             108                         if (this._settings.GetString("AnalyticsClientId") ==
                    "disabled")
                    @@ -149,6 +150,26 @@ public override ISite Site
149             150                 }
```

```
150  151            }
151  152
     153  +
     154  +         private void HandleEnableDtd(object sender, CancelEventArgs e)
     155  +         {
     156  +             if (!_settings.GetBoolean("DisableIgnoreDtdPrompt"))
     157  +             {
     158  +                 _settings["DisableIgnoreDtdPrompt"] = true;
     159  +                 var rc = MessageBox.Show("Enabling DTD processing has risks,
                          would you like to see the documentation on this?",
     160  +                     "DTD Processing Risk", MessageBoxButtons.YesNoCancel,
                          MessageBoxIcon.Warning);
     161  +                 if (rc == DialogResult.Cancel)
     162  +                 {
     163  +                     e.Cancel = true;
     164  +                 }
     165  +                 else if (rc == DialogResult.Yes)
     166  +                 {
     167  +                     WebBrowser.OpenUrl(this.Handle,
                          "https://microsoft.github.io/XmlNotepad/#help/validation/#dtd-entity-
                          leakage");
     168  +                     e.Cancel = true;
     169  +                 }
     170  +             }
     171  +         }
     172  +
152  173            private void OnButtonCancelClick(object sender, EventArgs e)
153  174            {
154  175                this.Close();
          @@ -240,6 +261,8 @@ public class UserSettings
240  261                private bool _promptOnReload;
241  262                private bool _attributesOnNewLine;
242  263
     264  +             public event EventHandler<CancelEventArgs> EnableDtdHandler;
     265  +
243  266                public UserSettings(Settings s)
244  267                {
245  268                    this._settings = s;
          @@ -317,7 +340,7 @@ internal void SaveColors()
```

```
                }

                public void Apply()
-               {
+               {
                    // and copy to cross-platform settings.
                    this._settings["FontFamily"] = this._font.FontFamily.Name;
                    this._settings["FontSize"] = (double)this._font.SizeInPoints;

@@ -370,7 +393,7 @@ public void Apply()
                    this._settings["MaximumLineLength"] =
this._maximumLineLength;
                    this._settings["MaximumValueLength"] =
this._maximumValueLength;
                    this._settings["AutoFormatLongLines"] =
this._autoFormatLongLines;
-                   this._settings["MaximumLineIndex"] = this._maximumLineIndex;
+                   this._settings["MaximumLineIndex"] = this._maximumLineIndex;
                    this._settings["IgnoreDTD"] = this._ignoreDTD;

                    this._settings["EnableXsltScripts"] =
this._enableXsltScripts;

@@ -700,7 +723,7 @@ public string UpdateFrequency
                        {
                            this._updateFrequency = newFrequency;
                        }
-                   }
+                   }
                    catch (FormatException)
                    {
                        throw new
Exception(StringResources.UpdateFrequencyFormatError);

@@ -915,6 +938,15 @@ public bool IgnoreDTD
                    }
                    set
                    {
+                       if (!value && this.EnableDtdHandler != null)
```

```
        942 +                    {
        943 +                        var args = new CancelEventArgs();
        944 +                        this.EnableDtdHandler(this, args);
        945 +                        if (args.Cancel)
        946 +                        {
        947 +                            return;
        948 +                        }
        949 +                    }
 918    950                         this._ignoreDTD = value;
 919    951                     }
 920    952                 }
            @@ -1058,7 +1090,7 @@ public bool XmlDiffHideIdentical
1058   1090                     get { return this._xmlDiffHideIdentical; }
1059   1091                     set { this._xmlDiffHideIdentical = value; }
1060   1092                 }
1061        -
        1093 +
1062   1094
1063   1095
1064   1096                 [SRCategory("EditingCategory")]
```

src/Model/Settings.cs

```
           @@ -1,4 +1,4 @@
   1       - using System;
       1   + using System;
   2   2     using System.Collections;
   3   3     using System.Collections.Generic;
   4   4     using System.ComponentModel;
           @@ -982,6 +982,7 @@ public void SetDefaults()
 982   982             this["AutoFormatLongLines"] = false;
 983   983
 984   984             this["IgnoreDTD"] = true;
       985   +         this["DisableIgnoreDtdPrompt"] = false;
 985   986             this["MaximumLineIndex"] = 1000000;
 986   987
 987   988             // XSLT options
```

src/Updates/Updates.xml

```
@@ -9,7 +9,7 @@
9  9
   <history>https://github.com/microsoft/XmlNotepad/blob/master/src/Updates/Updates.xml</history>
10 10     <frequency>1.00:00:00</frequency>
11 11   </application>
12    -  <version number="2.9.0.20">
   12 +  <version number="2.9.0.21">
13 13       <feature>Fix issue security advisory on DTD processing. Make default Ignore DTD option True, which is more secure.</feature>
14 14     </version>
15 15     <version number="2.9.0.17">
```

src/Version/Version.props

```
@@ -2,7 +2,7 @@
2  2  <Project ToolsVersion="12.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
3  3    <PropertyGroup>
4  4      <ApplicationRevision>0</ApplicationRevision>
5     -  <ApplicationVersion>2.9.0.20</ApplicationVersion>
   5  +  <ApplicationVersion>2.9.0.21</ApplicationVersion>
6  6      <Version>$(ApplicationVersion)</Version>
7  7      <Authors>Chris Lovett</Authors>
8  8      <Product>XmlNotepad</Product>
```

src/XmlNotepadSetup/Product.wxs

```
@@ -131,6 +131,15 @@
131 131      <Component Id="Employee.htm" Guid="3b3cc3ef-3ec0-42f1-a7a5-a23fad0886e3">
132 132        <File Id="Employee.htm" KeyPath="yes" />
133 133      </Component>
   134 +    <Component Id="DtdEntityExplosion.xml" Guid="edf58e5e-fe27-45e7-99da-98719bc7f643">
   135 +      <File Id="DtdEntityExplosion.xml" KeyPath="yes" />
   136 +    </Component>
```

```
                137 +       <Component Id="DtdEntityLeakage.xml" Guid="99c7e5d6-82bc-4c42-bec3-
                      cd8b546da124">
                138 +         <File Id="DtdEntityLeakage.xml" KeyPath="yes" />
                139 +       </Component>
                140 +       <Component Id="MaliciousDtd.dtd" Guid="bf188c6c-87f3-4d9f-8d4a-
                      cfd0a9e09c94">
                141 +         <File Id="MaliciousDtd.dtd" KeyPath="yes" />
                142 +       </Component>
134             143         </DirectoryRef>
135             144         <!-- shortcut in start menu -->
136             145         <DirectoryRef Id="ApplicationProgramsFolder">
                    @@ -171,6 +180,9 @@
171             180           <ComponentRef Id="rsspretty.xsl" />
172             181           <ComponentRef Id="willy.xsl" />
173             182           <ComponentRef Id="Employee.htm" />
                183 +         <ComponentRef Id="DtdEntityExplosion.xml" />
                184 +         <ComponentRef Id="DtdEntityLeakage.xml" />
                185 +         <ComponentRef Id="MaliciousDtd.dtd" />
174             186           <ComponentRef Id="ApplicationShortcut" />
175             187         </Feature>
176             188         <WixVariable Id="WixUILicenseRtf"
                      Value="$(var.Application.TargetDir)\license.rtf" />
```

Comments 0

Please sign in to comment.