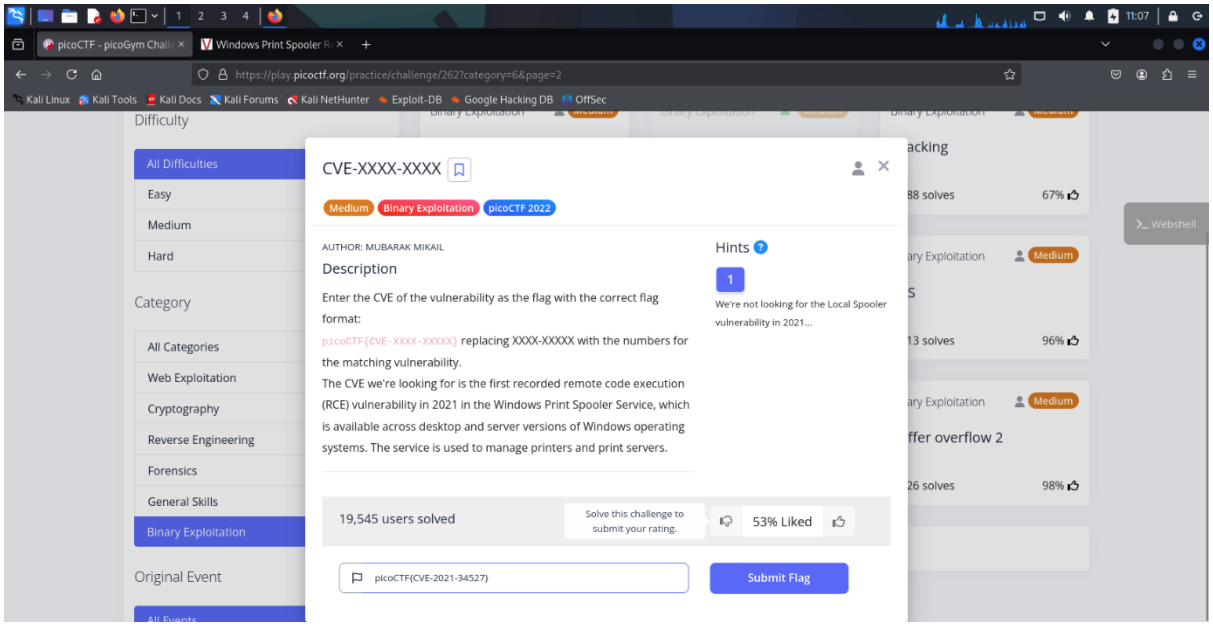
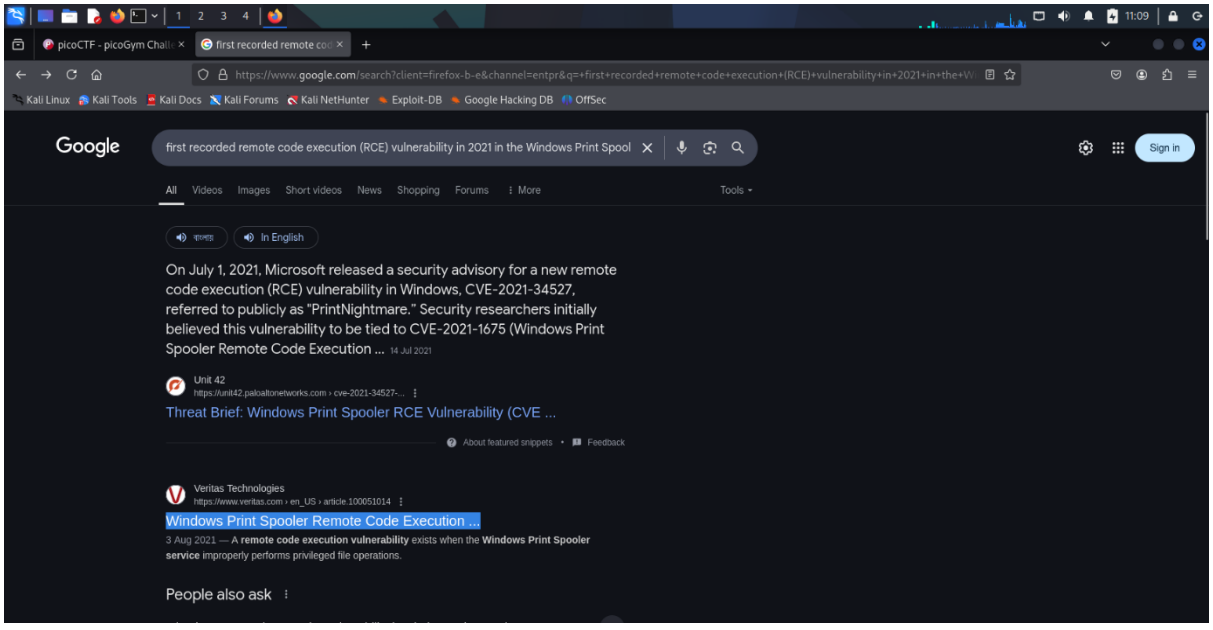
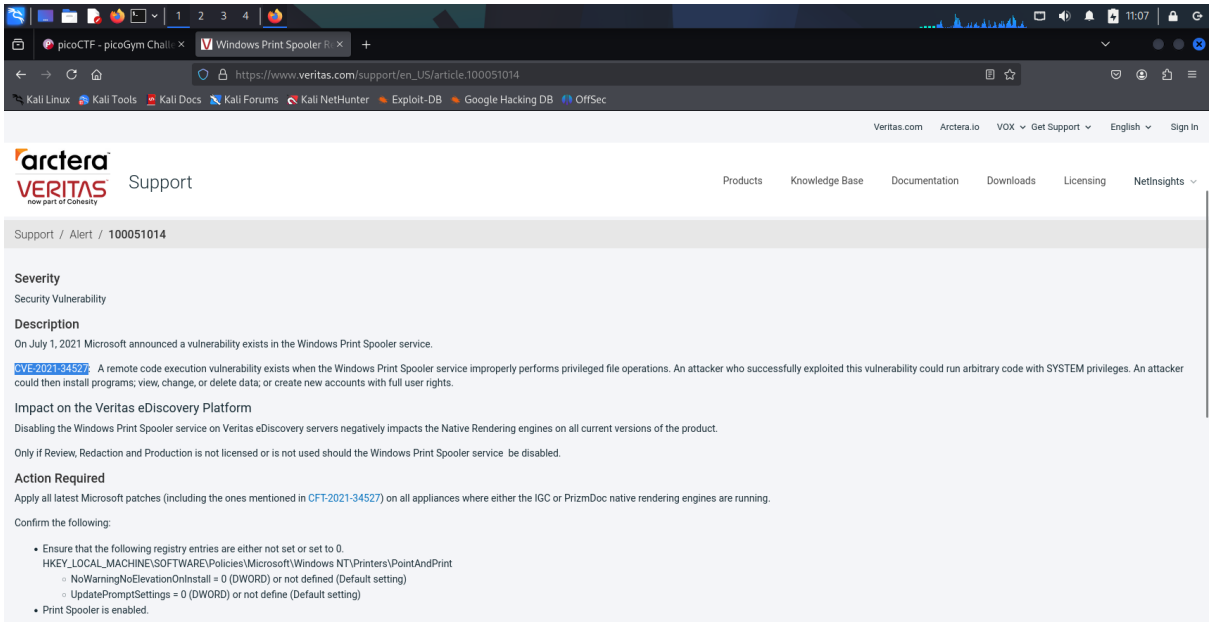

picoCTF - picoGym Challe
Windows Print Spooler R
https://play.picoctf.org/practice/challenge/262?category=6&page=2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Difficulty
All Difficulties
Easy
Medium
Hard
Category
All Categories
Web Exploitation
Cryptography
Reverse Engineering
Forensics
General Skills
Binary Exploitation
Original Event
CVE-XXXX-XXXX
Medium
Binary Exploitation
picoCTF 2022
AUTHOR: MUBARAK MIKAIL
Description
Enter the CVE of the vulnerability as the flag with the correct flag format:
picoCTF{CVE-XXXX-XXXXX} replacing XXXX-XXXXX with the numbers for the matching vulnerability.
The CVE we're looking for is the first recorded remote code execution (RCE) vulnerability in 2021 in the Windows Print Spooler Service, which is available across desktop and server versions of Windows operating systems. The service is used to manage printers and print servers.
Hints
1
We're not looking for the Local Spooler vulnerability in 2021...
19,545 users solved
Solve this challenge to submit your rating.
53% Liked
picoCTF{CVE-2021-34527}
Submit Flag
Webshell


picoCTF - picoGym Challe
first recorded remote cod
https://www.google.com/search?client=firefox-b-e&channel=entpr&q=+first+recorded+remote+code+execution+(RCE)+vulnerability+in+2021+in+the+W
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Google
first recorded remote code execution (RCE) vulnerability in 2021 in the Windows Print Spool
Sign in
All Videos Images Short videos News Shopping Forums More Tools
In English
On July 1, 2021, Microsoft released a security advisory for a new remote code execution (RCE) vulnerability in Windows, CVE-2021-34527, referred to publicly as "PrintNightmare." Security researchers initially believed this vulnerability to be tied to CVE-2021-1675 (Windows Print Spooler Remote Code Execution ... 14 Jul 2021
Unit 42
https://unit42.paloaltonetworks.com › cve-2021-34527-...
Threat Brief: Windows Print Spooler RCE Vulnerability (CVE ...
About featured snippets • Feedback
Veritas Technologies
https://www.veritas.com › en_US › article.100051014
Windows Print Spooler Remote Code Execution ...
3 Aug 2021 — A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations.
People also ask


picoCTF - picoGym Chall
Windows Print Spooler R
https://www.veritas.com/support/en_US/article.100051014
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Veritas.com
Arctera.io
VOX
Get Support
English
Sign In
arctera
VERITAS
now part of Cohesity
Support
Products
Knowledge Base
Documentation
Downloads
Licensing
NetInsights
Support / Alert / 100051014
Severity
Security Vulnerability
Description
On July 1, 2021 Microsoft announced a vulnerability exists in the Windows Print Spooler service.
CVE-2021-34527 A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
Impact on the Veritas eDiscovery Platform
Disabling the Windows Print Spooler service on Veritas eDiscovery servers negatively impacts the Native Rendering engines on all current versions of the product.
Only if Review, Redaction and Production is not licensed or is not used should the Windows Print Spooler service be disabled.
Action Required
Apply all latest Microsoft patches (including the ones mentioned in CFT-2021-34527) on all appliances where either the IGC or PrizmDoc native rendering engines are running.
Confirm the following:
Ensure that the following registry entries are either not set or set to 0.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (Default setting)
UpdatePromptSettings = 0 (DWORD) or not define (Default setting)
Print Spooler is enabled.