PrintNightmare

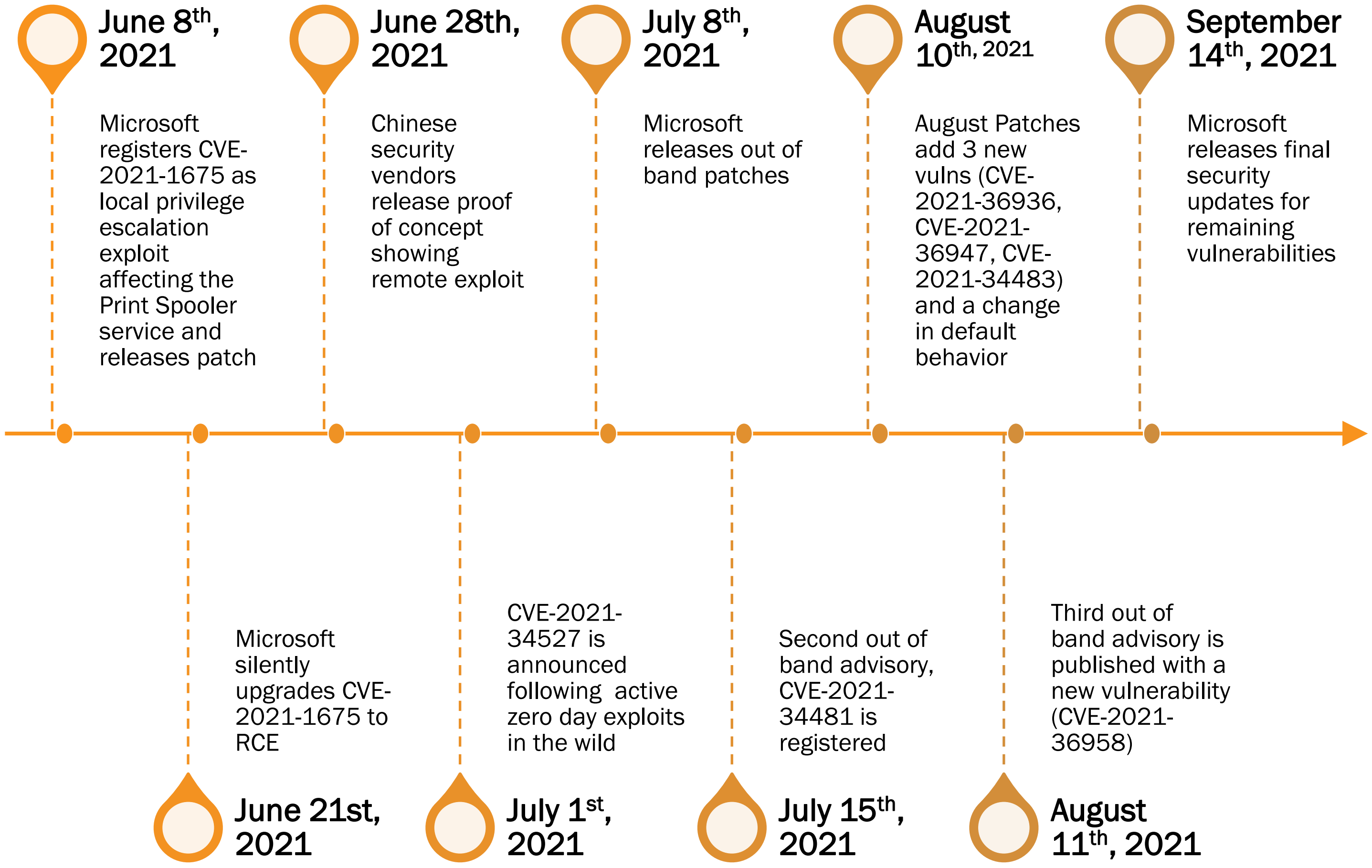
JEFF MALAVASI

Contents

- History
- Exploit Details
- Live Demo
- Mitigation/Protection
- Conclusion

History

Timeline



June 8th, 2021

Microsoft registers CVE-2021-1675 as local privilege escalation exploit affecting the Print Spooler service and releases patch

June 21st, 2021

Microsoft silently upgrades CVE-2021-1675 to RCE

June 28th, 2021

Chinese security vendors release proof of concept showing remote exploit

July 1st, 2021

CVE-2021-34527 is announced following active zero day exploits in the wild

July 8th, 2021

Microsoft releases out of band patches

July 15th, 2021

Second out of band advisory, CVE-2021-34481 is registered

August 10th, 2021

August Patches add 3 new vulns (CVE-2021-36936, CVE-2021-36947, CVE-2021-34483) and a change in default behavior

August 11th, 2021

Third out of band advisory is published with a new vulnerability (CVE-2021-36958)

September 14th, 2021

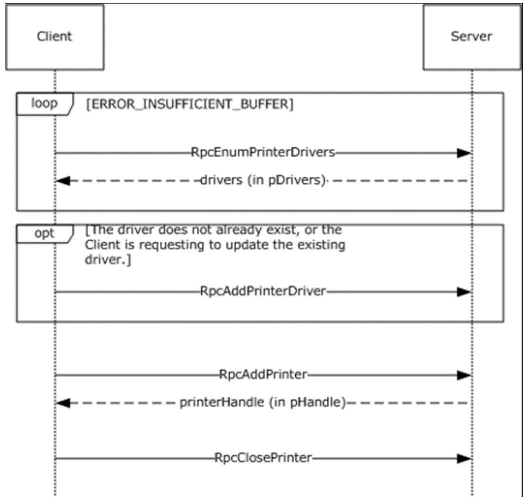
Microsoft releases final security updates for remaining vulnerabilities

From: [1]-[9]

Exploit

Microsoft Point and Print

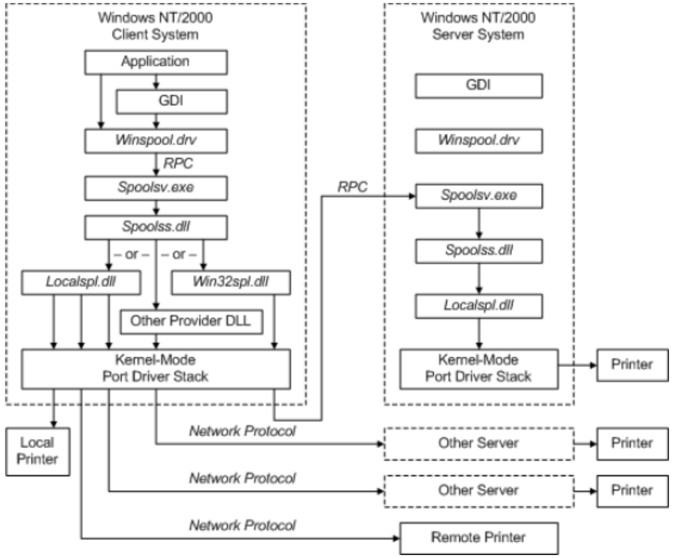
- Allows a user on a Windows client to connect to a printer remotely without installation media
- When a new printer is added to a client two actions occur:
  1. Driver and Queue associated files are downloaded from the server to the client
  2. Details regarding printer configuration parameters are also downloaded

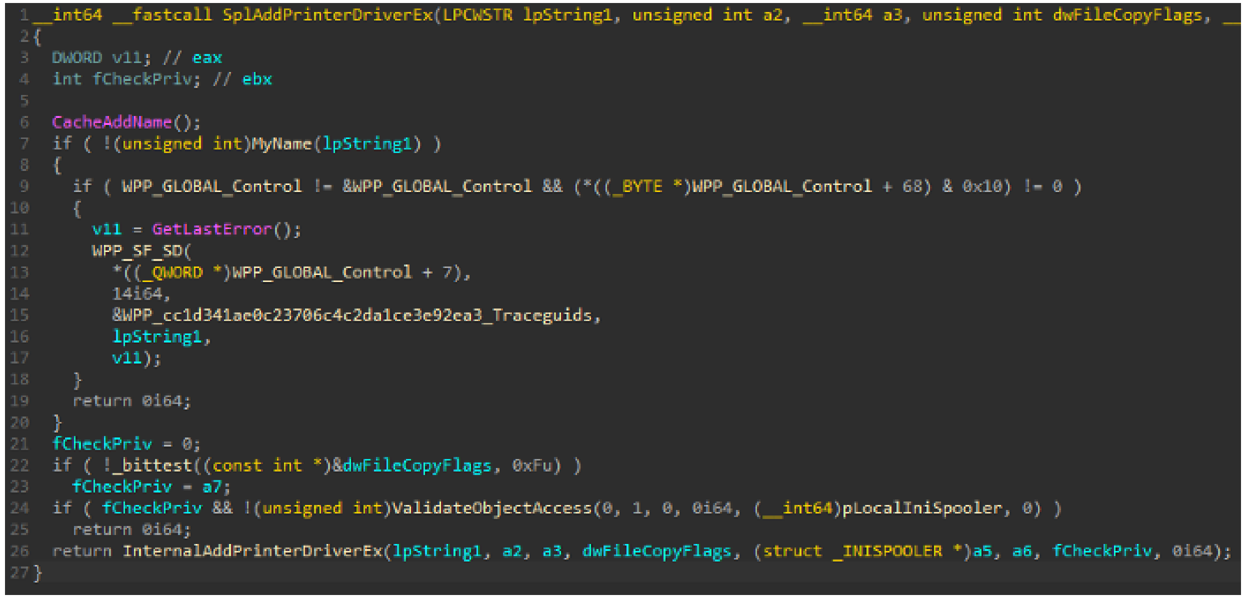

Client
Server
loop
[ERROR_INSUFFICIENT_BUFFER]
RpcEnumPrinterDrivers
drivers (in pDrivers)
opt
[The driver does not already exist, or the Client is requesting to update the existing driver.]
RpcAddPrinterDriver
RpcAddPrinter
printerHandle (in pHandle)
RpcClosePrinter

From: [10]-[11]

Privilege Escalation

- Logic flaw within Localspl.dll which is called by the Printer Spooler Service when loading a new print driver





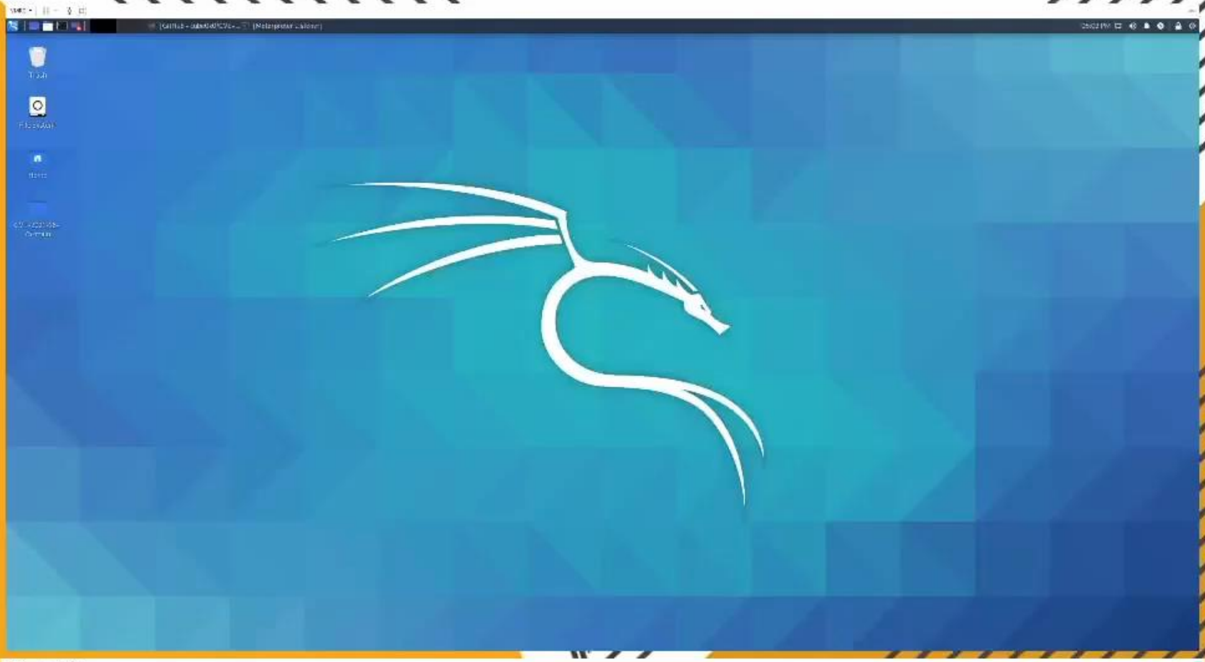
```
__int64 __fastcall SplAddPrinterDriverEx(LPCWSTR lpString1, unsigned int a2, __int64 a3, unsigned int dwFileCopyFlags, _
{
  DWORD v11; // eax
  int fCheckPriv; // ebx

  CacheAddName();
  if ( !(unsigned int)MyName(lpString1) )
  {
    if ( WPP_GLOBAL_Control != &WPP_GLOBAL_Control && (*((_BYTE *)WPP_GLOBAL_Control + 68) & 0x10) != 0 )
    {
      v11 = GetLastError();
      WPP_SF_SD(
        *((_QWORD *)WPP_GLOBAL_Control + 7),
        14i64,
        &WPP_cc1d341ae0c23706c4c2da1ce3e92ea3_Traceguids,
        lpString1,
        v11);
    }
    return 0i64;
  }
  fCheckPriv = 0;
  if ( !_bittest((const int *)&dwFileCopyFlags, 0xFu) )
    fCheckPriv = a7;
  if ( fCheckPriv && !(unsigned int)ValidateObjectAccess(0, 1, 0, 0i64, (__int64)pLocalIniSpooler, 0) )
    return 0i64;
  return InternalAddPrinterDriverEx(lpString1, a2, a3, dwFileCopyFlags, (struct _INISPOOLER *)a5, a6, fCheckPriv, 0i64);
}
```

From: [13]

Demo

Attacking Machine:
Kali Linux
Fake Printer
192.168.50.205



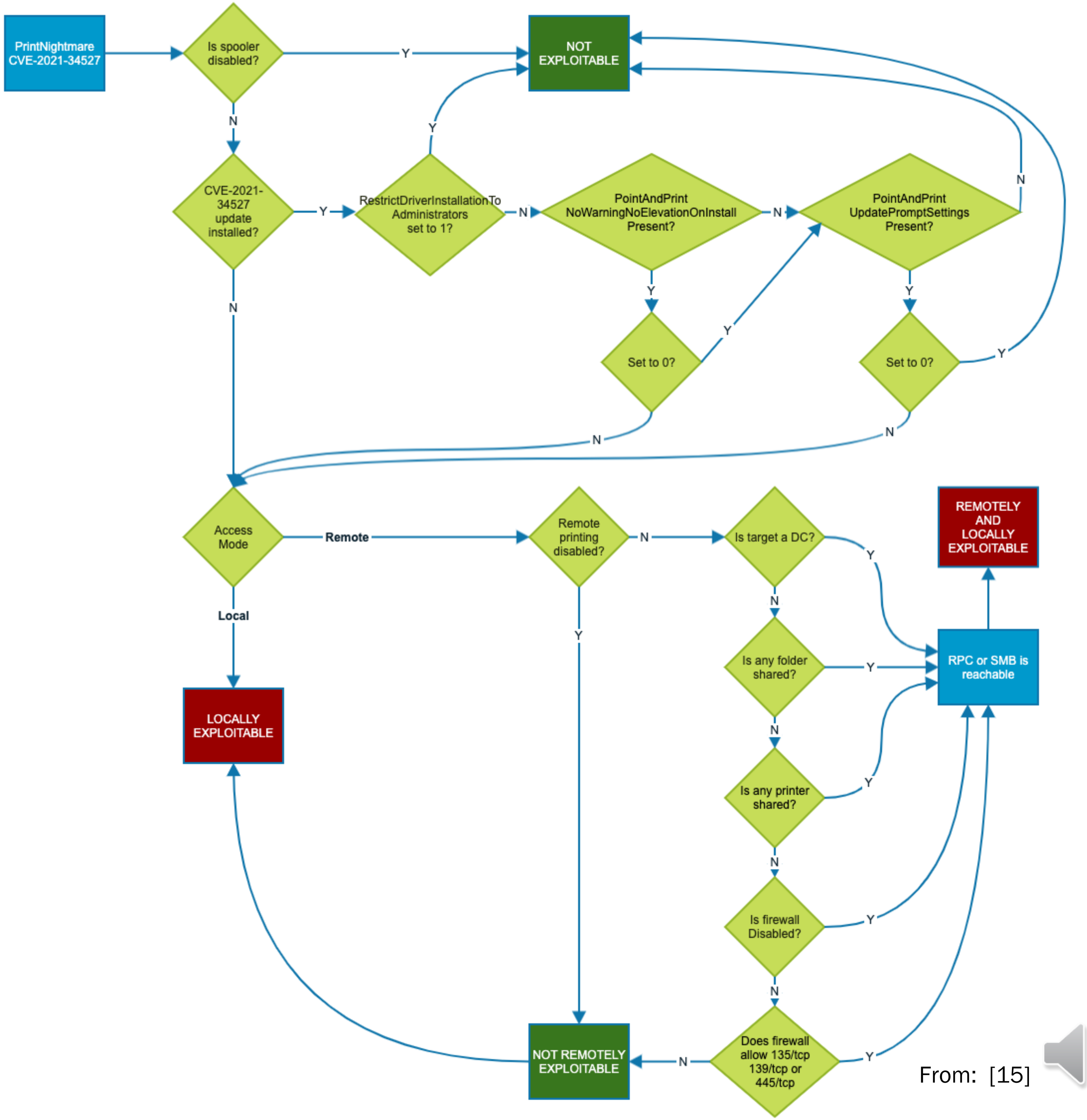
Target Machine:
Windows Server 2019
Domain Controller
192.168.50.128

PrintNightmare

JEFF MALAVASI

Mitigation

Vulnerability Workflow


PrintNightmare CVE-2021-34527
Is spooler disabled?
Y
N
NOT EXPLOITABLE
CVE-2021-34527 update installed?
Y
N
RestrictDriverInstallationTo Administrators set to 1?
Y
N
PointAndPrint NoWarningNoElevationOnInstall Present?
N
Y
PointAndPrint UpdatePromptSettings Present?
N
Y
Set to 0?
Y
N
Set to 0?
Y
N
Access Mode
Remote
Local
LOCALLY EXPLOITABLE
Remote printing disabled?
N
Y
Is target a DC?
Y
N
Is any folder shared?
Y
N
Is any printer shared?
Y
N
Is firewall Disabled?
Y
N
Does firewall allow 135/tcp 139/tcp or 445/tcp
Y
N
NOT REMOTELY EXPLOITABLE
RPC or SMB is reachable
REMOTELY AND LOCALLY EXPLOITABLE

From: [15]

Conclusion

- Limit the use of unnecessary services on critical infrastructure
- Block RPC and SMB with a host firewall
- Ensure UAC prompt is required, or restrict installation completely to administrators

References

1. “The PrintNightmare Continues: Another Zero-Day in Print Spooler Awaits Patch (CVE-2021-36958),” *Tenable®*, Aug. 19, 2021. https://www.tenable.com/blog/the-printnightmare-continues-another-zero-day-in-print-spooler-awaits-patch-cve-2021-36958 (accessed Nov. 21, 2021).
2. “CVE-2021-36958 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability.” https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958 (accessed Nov. 21, 2021).
3. “CVE-2021-36747 - Security Update Guide - Loading - Microsoft.” https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36947 (accessed Nov. 21, 2021).
4. “CVE-2021-36936 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability.” https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36936 (accessed Nov. 21, 2021).
5. “CVE-2021-34481 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability.” https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481 (accessed Nov. 21, 2021).
6. “CVE-2021-1675 - Security Update Guide - Microsoft - Windows Print Spooler Remote Code Execution Vulnerability.” https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675 (accessed Nov. 21, 2021).
7. “CVE-2021-34527 - Security Update Guide - Loading - Microsoft.” https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 (accessed Nov. 21, 2021).
8. “PrintNightmare Bug Exposes Domain Controllers,” *Lansweeper IT Asset Management*, Jul. 01, 2021. https://www.lansweeper.com/vulnerability/printnightmare-bug-exposes-domain-controllers/ (accessed Nov. 21, 2021).
9. “PrintNightmare Episode VI: Yet Another Print Spooler Vulnerability Disclosed,” *Lansweeper IT Asset Management*, Aug. 13, 2021. https://www.lansweeper.com/vulnerability/printnightmare-episode-6-yet-another-print-spooler-vulnerability-disclosed/ (accessed Nov. 21, 2021).
10. “Introduction to Point and Print - Windows drivers.” https://docs.microsoft.com/en-us/windows-hardware/drivers/print/introduction-to-point-and-print (accessed Nov. 21, 2021).
11. “[MS-RPRN]: Adding a Printer Driver to a Server.” https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/bc4d1830-8e1f-428a-9073-d655916494cf (accessed Nov. 21, 2021).
12. “[MS-RPRN]: Adding a Printer to a Server.” https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rprn/a33ebced-d8d5-44db-a728-7a77d0e40231 (accessed Nov. 21, 2021).
13. H. Cohen, “Understanding PrintNightmare Vulnerability,” *Medium*, Jul. 20, 2021. https://hidocohen.medium.com/understanding-printnightmare-vulnerability-cf4f1e0e506c (accessed Nov. 21, 2021).
14. The Cyber Mentor, *Print Nightmare AKA Domain Controller Domination*, (Aug. 04, 2021). Accessed: Nov. 21, 2021. [Online Video]. Available: https://www.youtube.com/watch?v=awQjEm0etO0
15. “CERT/CC Vulnerability Note VU#383432.” https://www.kb.cert.org (accessed Nov. 21, 2021).