



VDB-206880 · CVE-2022-2841

# CROWDSTRIKE FALCON 6.31.14505.0/6.42.15610 UNINSTALLATION AUTHORIZATION

CVSS Meta Temp Score ?

3.5

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.05

A vulnerability was found in CrowdStrike Falcon 6.31.14505.0/6.42.15610. It has been classified as problematic. Affected is some unknown functionality of the component *Uninstallation Handler*. The manipulation with an unknown input leads to a authorization vulnerability. CWE is classifying the issue as CWE-862. The software does not perform an authorization check when an actor attempts to access a resource or perform an action. This is going to have an impact on availability.

The weakness was published 08/22/2022 by Pascal Zenker and Max Moser with modzero AG as *Ridiculous vulnerability disclosure process with CrowdStrike Falcon Sensor*. The advisory is shared for download at modzero.com. This vulnerability is traded as CVE-2022-2841. Technical details are unknown but a public exploit is available.

A public exploit has been developed by Pascal Zenker/Max Moser. It is declared as functional. The exploit is shared for download at modzero.com. The vulnerability was handled as a non-public zero-day exploit for at least 54 days. During that time the estimated underground price was around \$0-\$5k.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

## Product

### Vendor

- CrowdStrike

### Name

- Falcon

## CPE 2.3

- 
- 

-----

## CPE 2.2

- 
- 

## Video

modzero Security Advisory [MZ-22-02]: Uninstall Protection Bypass for Crow...



[Open video](#) | [Show more videos](#)

## CVSSv3

VulDB Meta Base Score: 3.5

VulDB Meta Temp Score: 3.5

VulDB Base Score: 2.7

VulDB Temp Score: 2.6

VulDB Vector: 

VulDB Reliability: 


Researcher Base Score: 6.0

Researcher Vector: 

NVD Base Score: 2.7

NVD Vector: 

CNA Base Score: 2.7

CNA Vector (VulDB): 

# CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

## Exploiting

Class: Authorization

CWE: CWE-862 / CWE-863 / CWE-285

ATT&CK: Unknown

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Functional

Author: Pascal Zenker/Max Moser

Download: 🔒

EPSS Score: 🔒

EPSS Percentile: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

## Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

## Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🗝️

## Timeline

06/29/2022		Vendor informed
08/16/2022	+48 days	CVE reserved
08/22/2022	+6 days	Advisory disclosed
08/22/2022	+0 days	VulDB entry created
09/24/2022	+33 days	VulDB last update

## Sources

**Advisory:** Ridiculous vulnerability disclosure process with CrowdStrike Falcon Sensor

**Researcher:** Pascal Zenker/Max Moser

**Organization:** modzero AG

**Status:** Not defined

**CVE:** CVE-2022-2841 (🗝️)

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

## Entry

**Created:** 08/22/2022 10:01 AM

**Updated:** 09/24/2022 09:06 AM

**Changes:** 08/22/2022 10:01 AM (37), 08/22/2022 10:04 AM (19), 08/23/2022 07:45 AM (8), 09/24/2022 09:04 AM (2), 09/24/2022 09:06 AM (21)

**Complete:** 🔍

## Discussion

No comments yet. Languages: en.

Please log in to comment.