mod%log

modzero ag

2022-08-22

Ridiculous vulnerability disclosure process with CrowdStrike Falcon Sensor

Today, we publish a new advisory (https://www.modzero.com/advisories/MZ-22-02-CrowdStrike-FalconSensor.txt) for a vulnerability in the CrowdStrike (https://www.crowdstrike.com) Falcon Sensor, that was found by our team-mate Pascal Zenker (https://twitter.com/parzel2) as part of a recent red-teaming engagement.

The vulnerability is a case of insufficient control flow management (https://cwe.mitre.org/data/definitions/691.html), that allows an attacker with administrative privileges to bypass the *Falcon Agent Uninstall Protection* (https://www.crowdstrike.com/blog/tech-center/uninstall-protection-for-the-falcon-agent/) feature of CrowdStrike. As the exploit needs high privileges, the overall risk of the vulnerability is very limited.

While the vulnerability itself might not be worth a blog post, we'd like to write a few lines about the **ridiculous disclosure process**.

CrowdStrike is a major vendor in the area of IT security and we expected a straightforward coordinated disclosure process. To our surprise, the communication and disclosure with CrowdStrike was tedious and turned unprofessional in the end. Throughout the whole process, CrowdStrike pushed us repeatedly to disclose the vulnerability through their HackerOne (https://www.hackerone.com/) bug bounty program, which would have forced us to agree on the *HackerOne* Disclosure terms.

We communicated early on that we are neither willing to participate in any bug bounty program nor sign an NDA (https://en.wikipedia.org/wiki/Non-disclosure_agreement), because we are the ones, providing information to them. After providing CrowdStrike with a draft of the security advisory and exploit source code we were informed that they could not replicate the issue with an updated version of the sensor. Our request for a 14-day trial version to verify that ourselves was denied.

As the issue was not considered valid, we informed CrowdStrike that we would release the advisory to the public. In response, CrowdStrike tried again to set up a bug bounty disclosure meeting between "*modzero's Sr Leadership*" and CrowdStrike CISO "*[...] to discuss next steps related to **the** bug bounty disclosure*" in contrast to our previously stated disclosure rules.

Sometime later, we were able to acquire an updated version of the sensor and discovered that parts of the formerly provided exploit code and a specific *msiexec* call, are now flagged as malicious behaviour by the sensor. This leads us to conclude that CrowdStrike tried to "fix" the issue, while being told the issue didn't exist. Which is pretty **disrespectful** to us.

We were able to circumvent the countermeasures introduced silently by CrowdStrike. With small changes to the exploit, it is now working again (tested with version 6.42.15610 of the CrowdStrike Falcon software).

We believe that vulnerability disclosure is a two-way street. Vendors, as well as researchers, should act responsibly and show mutual goodwill and transparency. Mutual non-disclosure agreements and restrictions imposed by bug bounty programs limit the disclosure process. Remember, just because no CVE-IDs are publicly known, does not mean bugs haven't been reported and fixed. Many bug bounty reports never assign CVE-IDs, leading to a false perception of security and software quality.

References

- Proof of Concept screencast: https://youtu.be/3If-Fqwx-4s (https://youtu.be/3If-Fqwx-4s)

- modzero Security Advisory MZ-22-02: https://www.modzero.com/advisories/MZ-22-02-CrowdStrike-FalconSensor.txt (https://www.modzero.com/advisories/MZ-22-02-CrowdStrike-FalconSensor.txt)

Disclosure Timeline

```
2022/04    - Found vulnerability in CrowdStrike Falcon Sensor
             (6.31.14505.0)

2022/06/04 - modzero asked for security contact @ CrowdStrike,
             because their "report a security bug" page only refered
             to the hackerone Bug Bounty program.

2022/06/06 - CS answered that modzero can use the hackerone
             submission page, or send an E-Mail to their support at
             support@crowdstrike.com.

2022/06/06 - modzero asked if it is okay to send sensitive
             information about 0day vulnerabilities to support@.
             modzero also told CS that we are not willing to accept
             terms & conditions of hackerone, which is why we asked
             for a direct security contact.

2022/06/06 - CS offered to enroll modzero in a private bug bounty
             program at hackerone, under the conditions that we are
             willing to sign a mutual non-disclosure agreement.

2022/06/07 - to prevent further misunderstandings, modzero told CS
             again, that:

             * we would like to submit a security related bug.
             * we don't want to participate in any bug bounty
             programs.
             * we are not willing to sign any NDA because WE are the
             ones, providing information to CS.
             * we are not willing to accept any sort of terms &
             conditions that are out of scope of well known hacker
             ethics.
             * we only want to get a reliable security contact on
             their side.

             Aditionally, modzero sent a link to their current
             vulnerability disclosure policy.

2022/06/07 - CS told us to send the report to bugs@ for review.

2022/06/13 - CS asked for the report.

2022/06/13 - modzero told CS that we need a little bit more time to
             finish and double check everything before submitting.

2022/06/29 - modzero sent Security Advisory (draft), Proof of Concept
             exploit sourcecode, executable and a Screencast video of
             the PoC to CS.

2022/06/29 - CS told us, that we were testing using only an
             unsupported version of the Falcon Sensor. CS told us
             about the error message and that they are not able to
             reproduce.
```

2022/07/05 - modzero told CS that the error message can be ignored and refered to their PoC screencast video. We also asked for a recent (14-day trial) version of Falcon Sensor to provide reliable information if the most recent version is still vulnerable or not.

2022/07/05 - CS answered: "We do not provide trial licenses as part of this process, however having tested the PoC on our end with a modern sensor this does not appear to be a valid issue."

2022/07/05 - modzero announced publishing the advisory and exploit code by end of week, asking if the quote of CS "Having tested the PoC on our end with a modern sensor this does not appear to be a valid issue" can be used in our report.

2022/07/06 - CS asking for a meeting between modzero's Sr Leadership and CS to discuss next steps related to the bug bounty disclosure.

2022/07/07 - modzero, again, told CS, that we are not participating in any bug bounty program and that there is no need to discuss NDAs or bug bounty programs.

2022/08/12 - modzero managed to acquire a recent version (6.42.15610) of CrowdStrike Falcon and verified, that the attack is still possible. Furthermore, modzero figured out that the vulnerability (that was rejected by CrowdStrike first) has been silently fixed: The PoC that has been sent to CrowdStrike was flagged as malicious. The msiexec call of the deinstaller was also flagged as malicious. Both "countermeasures" can be circumvented easily, we updated the exploit accordingly.

2022/08/22 - modzero publishes Security Advisory and exploit code, because CrowdStrike was unwilling to set up a cooperative information exchange outside of their NDA-ridden BugBounty program to discuss vulnerabilities in their products.

Posted by modzero | **Permanent link (../../../../../archives/2022/08/22/ridiculous_vulnerability_disclosure_process_with_crowdstrike_falcon_sensor/index.html)** | File under: **security (../../../../../archives/security/index.html)**, **software (../../../../../archives/software/index.html)**, **hacking (../../../../../archives/hacking/index.html)**, **modzero (../../../../../archives/modzero/index.html)**, **exploit (../../../../../archives/exploit/index.html)**, **redteam (../../../../../archives/redteam/index.html)**, **rant (../../../../../archives/rant/index.html)**, **advisory (../../../../../archives/advisory/index.html)**