GREYNOISE

CISCO IOS XE

CONTENTS

Key Takeaways

In the dynamic landscape of cyber threats, the need for rapid and precise threat intelligence is paramount. GreyNoise is at the forefront, enhancing our sensor technology to deliver critical insights with unprecedented speed. Here's how our recent advancements are transforming threat detection and analysis:

- GreyNoise's new sensor framework uniquely allows us to rapidly respond and collect novel intelligence for emerging threats.
- With our new capabilities, Low/Medium/High-Interaction Honeypots Personas "appear" real to internet inventory services, allowing us to bait attackers targeting specific technologies. They can also be easily deployed in key IP space used by real businesses, making them attractive targets. The use of a customized low-interaction persona for Cisco IOS XE allowed our team to rapidly (within hours or days) adjust honeypots to capture new techniques.
- Using GreyNoise, the timeline for responding to actors and identifying novel exploitation techniques for emerging threats is faster, potentially reduced from weeks/months to hours and days, giving defenders a leg up against the adversaries.

Within 1 day and 30 minutes *of development, we were able to deploy a persona that baited attacks for CVE-2023-20198.*

Within 2 weeks *of just a single sensor deployment, we observed novel exploitation for the CVE and shared intelligence with partners.*

- CISA cites GreyNoise's work in their post "Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities"
- https://www.cisa.gov/guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities

Timeline

October 2023

10/16/2023 - Privilege Escalation CVE-2023-20198
Published for Cisco IOS XE

- We determine that the command injection vulnerability CVE-2021-1435 may be incorrectly attributed to exploitation activity in combination with CVE-2023-20198.
- We began working with partners to respond to this emerging threat.

10/17/2023 - GreyNoise Developed Low-Interaction Cisco IOS XE Personas

- We create a Cisco IOS XE persona in about 30 minutes.
- We strategically deploy the low-interaction persona to a single IP in AWS, knowing that we are correctly presenting as a Cisco IOS XE device.

10/19/2023 - GreyNoise confirms that an un-tracked command injection CVE is involved

- In partnership with VulnCheck, GreyNoise bisects patches and produces a PoC for CVE-2019-xxxx command injection vulnerabilities.
- Between public information and private information, we accurately ascertain that CVE-2021-1435 is not involved in the active exploitation campaign.
  - https://www.greynoise.io/blog/unpacking-cve-2023-20198-a-critical-weakness-in-cisco-ios-xe
- A GreyNoise tag is released to track older command injection vulns.
  - https://viz.greynoise.io/tag/cisco-ios-xe-rce-attempt?days=3

10/20/2023 - GreyNoise tag for Privilege Escalation CVE-2023-20198 released

- The scope of vulnerability and mechanisms that may be used for signature bypasses are captured.
  - https://nginx.org/en/docs/http/ngx_http_core_module.html#location
- A GreyNoise tag is released to track CVE-2023-20198.
  - https://viz.greynoise.io/tag/cisco-ios-xe-privilege-escalation-attempt?days=3

October 2023

10/23/2023 - GreyNoise collaborates with the community

- GreyNoise advocates for the successful removal of CVE-2021-1435 from CISA's KEV.

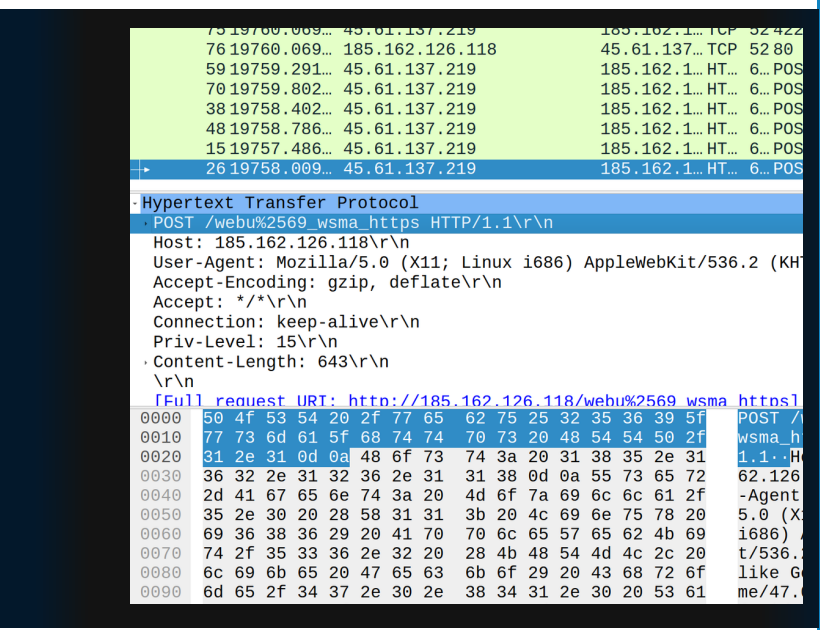
10/31/2023 - GreyNoise observes novel exploitation of CVE-2023-20198 with our new sensor

- The observed payload utilizes predicted signature bypass mechanisms, as noted on 10/20

```
POST /%2577eb%2575i_%2577sma_Http HTTP/1.1
Host: 45.93.95.6:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.93 Safari/537.36
Connection: close
Content-Length: 720
Accept-Encoding: gzip

<?xml version="1.0"?> <SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://
schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"> <SOAP:Header> <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext">
<wsse:UsernameToken SOAP:mustUnderstand="false"> <wsse:Username>admin</wsse:Username><wsse:Password>*****</
wsse:Password></wsse:UsernameToken></wsse:Security></SOAP:Header><SOAP:Body><request correlator="exec1"
xmlns="urn:cisco:wsma-exec"> <execCLI xsd="false"><cmd>uname -a</cmd><dialogue><expect></expect><reply></reply></dialogue></
execCLI></request></SOAP:Body></SOAP:Envelope>
```

November 2023



11/01/2023 - GreyNoise shares PCAP, intelligence, and analysis with partners

- Noted that we have observed novel exploitation that uses varying capitalization, _http(s), and double URL-Encoding.
- Noted that the number of possible payload variations that can result in successful exploitation are massive.
- Noted that for the performance of network signatures attempting to match all variations, a "behavior-first" signature can be crafted using public documentation.
  - HTTP POST lacking well-defined authentication methods.
    - https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/restapi/restapi/RESTAPIclient.html
  - POST body containing well-defined Cisco XML SOAP schema.
  - Then, perform computationally expensive operations to match indicators for the webui_wsma_http(s) variations.

November 2023

11/06/2023 - Metasploit published exploitation modules with additional check

- https://github.com/sfewer-r7/metasploit-framework/blob/64c9968328ac452913bb7850140a1b70ba2109bb/modules/exploits/linux/misc/cisco_ios_xe_rce.rb#L132

11/07/2023 - GreyNoise pushes a Cisco IOS XE persona update to match additional Metasploit checks

- Persona now shows as vulnerable to the Metasploit module.

Case Study: CISCO IOS XE

About GreyNoise

GreyNoise helps security teams focus on threats that really matter, and ignore the ones that don't. We collect, analyze and label data on IP addresses that scan and attack the entire internet, saturating security teams with alerts. This unique perspective helps analysts focus their time on targeted and emerging threats, and waste less time on irrelevant or harmless activity.

Get started for free ↗

Schedule a demo ↗