

Dateline: 2023-10-17



S T O R M ⚡ W A T C H

<https://www.greynoise.io/resources/storm-watch-weekly-livestream>



Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (<https://www.greynoise.io>), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

<https://stormwatch.libsyn.com/>

<https://discord.com/channels/1092816662241222676/1159560723412811847>



Storm ⚡ Watch

https://www.theregister.com/2023/10/10/october_2023_patch_tuesday/



SMH

Folks who use Microsoft Defender for Office are protected from attachments that attempt to exploit this vulnerability.

In current attack chains, the use of the Block all Office applications from creating child processes Attack Surface Reduction Rule will prevent the vulnerability from being exploited.

Organizations who cannot take advantage of these protections can add `Wordpad.exe` to this registry key as values of type `REG_DWORD` with data `1`

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
  Internet Explorer\Main\FeatureControl\
    FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION
```

<https://nvd.nist.gov/vuln/detail/CVE-2023-36884>

"WordPad is no longer being updated and will be removed in a future release of Windows"


<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>

<https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/>

 Cisco Security Advisory

Cisco IOS XE Software Web UI Privilege Escalation Vulnerability



Advisory ID: cisco-sa-iosxe-webui-privesc-j22SaA4z CVE-2023-20198
First Published: 2023 October 16 15:00 GMT
Last Updated: 2023 October 16 21:11 GMT
Version 1.1: [Interim](#)
Workarounds: No workarounds available
Cisco Bug IDs: [CSCwh87343](#)
CVSS Score: [Base 10.0](#) 

[Download CSAF](#)

[Download CVRF](#)

[Email](#)

Summary

Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

[Subscribe](#)

Related to This Advisory

<https://viz.greynoise.io/tag/cisco-ios-xe-cve-2023-20198-scanner?days=30>

Your Rating:



Leveraging existing detections, we observed the actor exploiting **CVE-2021-1435**, for which Cisco provided a patch in 2021, to install the implant after gaining access to the device. We have also seen devices fully patched against CVE-2021-1435 getting the implant successfully installed through an as of yet undetermined mechanism.

Organizations should look for unexplained or newly created users on devices as evidence of potentially malicious activity relating to this threat. One method to identify if the implant is present is to run the following command against the device, where the "DEVICEIP" portion is a placeholder for the IP address of the device to check:

```
curl -k -X POST "https[:]//DEVICEIP/webui/logoutconfirm.html?logon_hash=1"
```

<https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/>

[← Go back](#)<https://vulncheck.com/blog/cisco-implants>

October 17, 2023

Wilderness: Cisco IOS XE Implant in the Wild

Key Takeaways

- ✓ CVE-2023-20198 appears to have been widely exploited to install implants on Cisco IOS XE systems.
- ✓ VulnCheck performed an internet-scan and found thousands of implanted hosts.
- ✓ VulnCheck released a scanner to detect the implant on affected devices.

On October 16, 2023 Cisco disclosed an authentication bypass, CVE-2023-20198, affecting Cisco IOS XE. The disclosure reported that the vulnerability had been exploited in the wild to help install implants on affected switches and routers. Additionally, Cisco shared a simple technique to determine if an IOS XE

<https://github.com/vulncheck-oss/cisco-ios-xe-implant-scanner>

```
1 $ curl -X POST http://192.168.1.1/webui/logoutconfirm.html?logon_hash=1
2 1a80b7389ccd0a5dab
```



tags:"Cisco IOS XE CVE-2023-20198 Scanner"

> UNKNOWN HOSTING

176.58.124.134

ORGANIZATION: Akamai **LINODE** ed Cloud ACTOR: unknown LAST SEEN: 2023-10-17

SOURCE: United Kingdom DESTINATION: United States, United Kingdom, Switzerland, Ukraine, Latvia + 7
More

⚡ CISCO IOS XE CVE-2023-20198 SCANNER

⚡ TLS/SSL CRAWLER

⚡ WEB CRAWLER

🔗 ZMAP CLIENT

<https://viz.greynoise.io/query?gnql=tags:%22Cisco%20IOS%20XE%20CVE-2023-20198%20Scanner%22>

<https://people.redhat.com/~hkario/marvin/#mitigation>

The Marvin Attack is a return of a 25 year old vulnerability that allows performing RSA decryption and signing operations as an attacker with the ability to observe only the time of the decryption operation performed with the private key.



<https://people.redhat.com/~hkario/marvin/#mitigation>



In 1998, Daniel Bleichenbacher discovered that the error messages given by SSL servers for errors in the PKCS #1 v1.5 padding allowed an adaptive-chosen ciphertext attack; this attack fully breaks the confidentiality of TLS when used with RSA encryption. In 2018 (19 years later) many internet servers were still vulnerable to slight variations of the original attack.

<https://people.redhat.com/~hkario/marvin/#mitigation>

We show that many implementations previously thought immune, are vulnerable to the timing variant of the same attack.

While the main venue of attack are TLS servers, the core issues that caused its wide spread are applicable to most asymmetric cryptographic algorithms (Diffie-Hellman, ECDSA, etc.), not just to RSA. Lessons learned are also applicable to testing the majority of cryptographic algorithms that can be vulnerable to side-channel attacks, not just public key cryptography.



GREYNOISE
LABS

CVE-2023-4421/5388: NSS (TLS level) [Not a complete fix]

CVE-2023-0361: GnuTLS (TLS level)

CVE-2022-4304: OpenSSL (TLS level)

CVE-2020-25657: M2Crypto [ineffective, requires OpenSSL fix]

CVE-2020-25659: pyca/cryptography [ineffective, requires OpenSSL fix]

no CVE: OpenSSL-ibmca

no CVE: OpenSSL (API level)

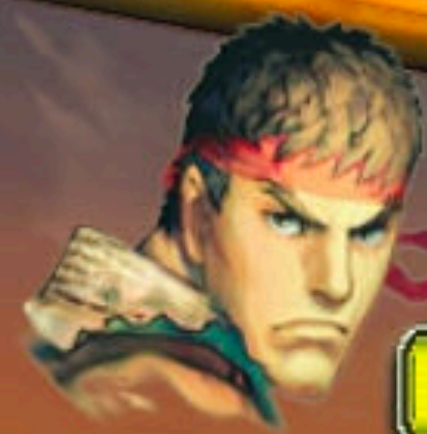
Go: crypto/rsa DecryptPKCS1v15SessionKey(limited leakage)

GNU MP: mpz_powm_sec (leaks zero high order bits in result)

<https://people.redhat.com/~hkario/marvin/#mitigation>

Infosec Influencer

Fighter



PLAYER 1

SCORE 00094800

K.O.
99

PRESS 2P START

CPU



SIGNAL O-DAY

FAKE NEWS

FINAL

REVENGE

COMBO

COMBO

REVENGE

COMBO

COMBO



PSA: we have seen the vague viral reports alleging a Signal 0-day vulnerability.

After responsible investigation *we have no evidence that suggests this vulnerability is real* nor has any additional info been shared via our official reporting channels.

BLOG

<https://censys.com/http-who-cve-2023-44487/>

HTTP/Who? CVE-2023-44487

BLOG

<https://censys.com/red-herrings-and-honeypots/>

Unmasking Deception: Navigating Red Herrings and Honeypots



VULNERABILITIES

CVE-2023-22515: Critical Privilege Escalation Vulnerability in Atlassian's Confluence

Glenn Thorpe | October 10, 2023



<https://www.greynoise.io/blog/cve-2023-22515-critical-privilege-escalation-vulnerability-in-atlassians-confluence>

VULNERABILITIES

CVE-2023-38545: So you cURL, but will you cIRL?

On October 11th, 2023, a heap-based buffer overflow in curl was disclosed under the identifier CVE-2023-38545. The vulnerability affects libcurl 7.69.0 to and including 8.3.0. Vulnerable versions of libcurl may be embedded in existing applications. However, to reach the vulnerable code path, the application must be configured to utilize one of the SOCKS5 proxy modes and attempt to resolve a hostname with extraneous length.

Matthew Remaille | Oct 11, 2023



<https://www.greynoise.io/blog/cve-2023-38545-so-you-curl-but-will-you-cirl>



GREYNOISE
LABS

STORM ⚡ WATCH



Don't click that link!
Don't reuse passwords!
Don't plug-in random USB sticks!
Don't use a flat network!
Don't use cloud apps!

- 🏷️ Cisco IOS XE CVE-2023-20198 Scanner
- 🏷️ Fortinet FortiSIEM Command Injection Attempt
- 🏷️ Fortinet FortiWLM Command Injection Attempt
- 🏷️ Jira Data Exposure Scanner
- 🏷️ SharePoint CVE-2023-29357 Check
- 🏷️ Atlassian Confluence Server Scanner
- 🏷️ SOCKS5 Proxy Scanner
- 🏷️ cURL/libcurl Heap Buffer Overflow Attempt

<https://viz.greynoise.io/trends?view=recent>

It Has Been

1

Days Since The
Last KEV Release

<https://observablehq.com/@greynoise/greynoise-tags>

2023-10-10: Adobe Acrobat and Reader Use-After-Free Vulnerability

2023-10-10: Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability

2023-10-10: Microsoft Skype for Business Privilege Escalation Vulnerability

2023-10-10: Microsoft WordPad Information Disclosure Vulnerability

2023-10-10: HTTP/2 Rapid Reset Attack Vulnerability

2023-10-16: Cisco IOS XE Web UI Privilege Escalation Vulnerability

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

<https://kevin.gtfkd.com/>

Welcome to the KEVIN API

An API for accessing CISA's Known Exploited Vulnerabilities Catalog (KEV) and CVE Data

Dark Theme

[Go to Examples](#)

Number of CVEs:

287,072

Number of KEVs:

1,024

[KEV API Usage](#)

/kev Usage

- [/kev](#) - Get the most recently added KEVs
- [/kev?page=1&per_page=25](#) - Get the first 25 Known Exploited Vulnerabilities (default pagination)
- [/kev?page=2&per_page=25](#) - Get the next 25 Known Exploited Vulnerabilities (default pagination)
- [/kev?search=Microsoft&page=1&per_page=10](#) - Search KEV based on description (first 10 results)
- [/kev/CVE-ID](#) - Fetch a KEV by CVE-ID
- [/kev/recent?days=7](#) - Get new vulnerabilities added in the last 7 days
- [/kev?sort=date&order=desc&page=1&per_page=15](#) - Sort first 15 KEV by date added (newest first)
- [/kev?sort=severity&order=desc&page=1&per_page=15](#) - Sort first 15 KEV by NVD baseScore in descending order (highest scores first)

[Vuln API Usage](#)

<https://github.com/synfinner/KEVIN>

/vuln Usage



```
{
  "title": "CISA Catalog of Known Exploited Vulnerabilities",
  "catalogVersion": "2023.10.16",
  "dateReleased": "2023-10-16T15:00:10.5444Z",
  "count": 1020,
  "vulnerabilities": [
    {
      "cveID": "CVE-2021-27104",
      "vendorProject": "Accellion",
      "product": "FTA",
      "vulnerabilityName": "Accellion FTA OS Command Injection Vulnerability",
      "dateAdded": "2021-11-03",
      "shortDescription": "Accellion FTA contains ...",
      "requiredAction": "Apply updates per vendor instructions.",
      "dueDate": "2021-11-17",
      "knownRansomwareCampaignUse": "Known",
      "notes": ""
    }
  ]
}
```

<https://observablehq.com/@greynoise/cisa-kev-ransomware-cves>

<https://discord.com/channels/1092816662241222676/1159560723412811847>



Storm ⚡ Watch



Dateline: 2023-10-17



S T O R M ⚡ W A T C H