19 EKİM 2023

ZERO DAY

Cisco'nun ağ cihazları için geliştirdiği işletim sistemi Cisco IOS XE'nin aktif olarak istismar edilen maksimum önem derecesine sahip güvenlik açığı yayınlandı.

CİSCO IOS XE YAZILIMI WEB KULLANICI ARAYÜZÜ AYRICALIK YÜKSELTME GÜVENLİK AÇIĞI

CVE: CVE-2023-20198

CVSS Puanı: 10

Referanslar:
https://www.tenable.com/blog/cve-2023-20198-zero-day-vulnerability-in-cisco-ios-xe-exploited-in-the-wild
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
https://nvd.nist.gov/vuln/detail/CVE-2023-20198

Açıklama:
Cisco'nun Talos birimi, CVE-2023-20198'i hedef alan saldırıların izlerini ilk olarak 28 Eylül'de belirlediklerini ve ilgili etkinliğin 18 Eylül'e kadar uzandığını açıkladı.
Güvenlik açığı, uzaktaki, kimliği doğrulanmamış bir saldırganın etkilenen sistemde "ayrıcalık düzeyi 15" (tüm komutlara tam erişim) erişimine sahip bir hesap oluşturmasına olanak tanır. Saldırgan daha sonra etkilenen sistemin kontrolünü ele geçirmek için bu hesabı kullanabilir.

Cisco IOS XE Yazılımının web kullanıcı arayüzü özelliği etkinse bu güvenlik açığından etkilenebilir.
Web kullanıcı arayüzü özelliği ip http sunucusu veya ip http secure-server komutları aracılığıyla etkinleştirilir .

ip http sunucusu komutu mevcutsa ve yapılandırma aynı zamanda ip http active-session-modules none içeriyorsa , güvenlik açığından HTTP üzerinden yararlanılamaz.
ip http secure-server komutu mevcutsa ve yapılandırma aynı zamanda ip http secure-active-session-modules none içeriyorsa , güvenlik açığından HTTPS üzerinden yararlanılamaz.

Cisco, müşterilerin internete bakan tüm sistemlerde HTTP Sunucusu özelliğini devre dışı bırakmasını tavsiye etmektedir.
HTTP Sunucusu özelliğini devre dışı bırakmak için genel yapılandırma modunda no ip http sunucusu veya no ip http secure-server komutunu kullanılır. Hem HTTP sunucusu hem de HTTPS sunucusu kullanılıyorsa, HTTP Sunucusu özelliğini devre dışı bırakmak için her iki komutun da kullanılması gerekir.