Více chyb zabezpečení ve funkci webového uživatelského rozhraní softwaru Cisco IOS XE

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

Cisco Security Advisory

souhrn

Společnost Cisco poskytuje aktualizaci pro probíhající vyšetřování pozorovaného využívání funkce webového uživatelského rozhraní v softwaru Cisco IOS XE. Poskytujeme vylepšenou detekci přítomnosti implantátu.

Cisco aktualizuje informační zprávu, jakmile budou další verze zveřejněny v Cisco Software Download Center. Informace o opravách lze nalézt v části Opravený software tohoto informačního bulletinu.

Naše vyšetřování ukázalo, že herci zneužili dva dříve neznámé problémy.

Útočník nejprve zneužil CVE-2023-20198 k získání počátečního přístupu a vydal příkaz s oprávněním 15 k vytvoření kombinace místního uživatele a hesla. To umožnilo uživateli přihlásit se s běžným uživatelským přístupem.

Útočník poté zneužil další součást webového uživatelského rozhraní a využil nového místního uživatele ke zvýšení oprávnění rootovat *a* zapsat implantát do systému souborů. Společnost Cisco tomuto problému přiřadila CVE-2023-20273.

- **CVE-2023-20198** bylo přiděleno skóre CVSS 10,0.
- **CVE-2023-20273** bylo přiděleno CVSS skóre 7,2.

Obě tyto CVE jsou sledovány CSCwh87343 .

Kroky k uzavření vektoru útoku pro tyto chyby zabezpečení naleznete v části Doporučení tohoto informačního zpravodaje.

Toto doporučení je k dispozici na následujícím odkazu: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Dotčené produkty

Zranitelné produkty

Tyto chyby zabezpečení ovlivňují software Cisco IOS XE, pokud je povolena funkce webového uživatelského rozhraní. Funkce webového uživatelského rozhraní je povolena prostřednictvím příkazů **ip http server** nebo **ip http secure-server** .

Určete konfiguraci serveru HTTP

Chcete-li zjistit, zda je pro systém povolena funkce HTTP Server, přihlaste se do systému a použijte příkaz **show running-config | zahrňte příkaz ip http server|secure|active** do CLI, abyste zkontrolovali přítomnost příkazu **ip http serveru** nebo příkazu **ip http secure-server** v globální konfiguraci. Pokud je přítomen některý z příkazů, je pro systém povolena funkce HTTP Server.

Následující příklad ukazuje výstup show **running-config | include ip http server|secure|active** příkaz pro systém, který má povolenou funkci HTTP Server:

```
Router# show running-config | zahrnout ip http
server|zabezpečený|aktivní
 ip http server
ip http zabezpečený-server
```

Poznámka: Přítomnost jednoho nebo obou příkazů v konfiguraci systému znamená, že je povolena funkce webového uživatelského rozhraní.

Pokud je přítomen příkaz **ip http server** a konfigurace obsahuje také **ip http active-session-modules none** , tyto chyby zabezpečení nelze přes HTTP zneužít.

Pokud je přítomen příkaz **ip http secure-server** a konfigurace obsahuje také **ip http secure-active-session-modules none** , tyto chyby zabezpečení nelze přes HTTPS zneužít.

Produkty potvrzeno, že nejsou zranitelné

Tyto chyby zabezpečení se týkají pouze produktů uvedených v části Zranitelné produkty tohoto informačního bulletinu.

Podrobnosti

Webové uživatelské rozhraní je vestavěný nástroj pro správu systému založený na grafickém uživatelském rozhraní, který poskytuje možnost zřídit systém, zjednodušit nasazení a správu systému a zlepšit uživatelskou zkušenost. Dodává se s výchozím obrazem, takže není potřeba nic povolovat ani instalovat žádnou licenci do systému. Webové uživatelské rozhraní lze použít k vytváření konfigurací i ke sledování a odstraňování problémů systému bez odborných znalostí CLI.

Ukazatele kompromisu

Chcete-li zjistit, zda mohl být systém ohrožen, proveďte následující kontroly:

Zkontrolujte systémové protokoly, zda neobsahuje některou z následujících zpráv protokolu, kde ***uživatel*** může být **cisco_tac_admin** , **cisco_support** nebo jakýkoli nakonfigurovaný místní uživatel, kterého správce sítě nezná:

```
%SYS-5-CONFIG_P: Nakonfigurováno programově procesem SEP_webui_wsma_http
z konzole jako uživatel na řádku

 %SEC_LOGIN-5-WEBLOGIN_SUCCESS: Úspěšné přihlášení [uživatel: uživatel ]
[Zdroj: zdrojová_IP_adresa ] v 03:42:13 UTC St 20. října 12 11
```

Poznámka : Zpráva **%SYS-5-CONFIG_P** bude přítomna pro každou instanci, kdy uživatel přistoupil k webovému uživatelskému rozhraní. Indikátor, který je třeba hledat, jsou nová nebo neznámá uživatelská jména přítomná ve zprávě.

Zkontrolujte systémové protokoly, zda neobsahuje následující zprávu, kde ***název_souboru*** je neznámý název souboru, který nekoreluje s očekávanou akcí instalace souboru:

```
%WEBUI-6-INSTALL_OPERATION_INFO: Uživatel: uživatelské jméno , Operace
instalace: PŘIDAT název souboru
```

Společnost Cisco Talos poskytla následující příkaz ke kontrole přítomnosti implantátu, kde ***systemip*** je IP adresa systému, který se má zkontrolovat. Tento příkaz by měl být vydán z pracovní stanice s přístupem k příslušnému systému:

```
curl -k -H "Oprávnění: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST
"https:// systemip /webui/logoutconfirm.html?logon_hash=1"
```

Pokud požadavek vrátí hexadecimální řetězec, například **0123456789abcdef01** , implantát je přítomen.

Poznámka : Výše uvedený příkaz by měl být zadán jako jeden příkazový řádek.

Poznámka : Pokud je systém nakonfigurován pouze pro přístup HTTP, použijte schéma HTTP v příkladu příkazu.

Pro detekci zneužití jsou k dispozici také následující ID pravidel Snort:

- 3:50118 – upozornění na počáteční injekci implantátu (CVE-2023-20273)
- 3:62527 - upozornění na interakci implantátu
- 3:62528 - upozornění na interakci implantátu
- 3:62529 - upozornění na interakci implantátu
- 3:62541 – upozornění na pokus o zneužití pro počáteční přístup (CVE-2023-20198)
- 3:62542 – upozornění na pokus o zneužití pro počáteční přístup (CVE-2023-20198)

Řešení

Neexistují žádná zástupná řešení, která by tyto chyby zabezpečení řešila.

Deaktivace funkce HTTP Server eliminuje vektor útoku pro tyto chyby zabezpečení a může být vhodným zmírněním, dokud nebude možné upgradovat postižená zařízení. Správci mohou zakázat funkci HTTP Server pomocí příkazu **no ip http server** nebo **no ip http secure-server** v režimu globální konfigurace. Pokud se používá *server http* i *server HTTP , pak jsou k deaktivaci funkce HTTP Server vyžadovány oba příkazy.*

Omezení přístupu k serveru HTTP na důvěryhodné sítě omezí vystavení těmto chybám zabezpečení. Následující příklad ukazuje, jak povolit vzdálený přístup k serveru HTTP z důvěryhodné sítě 192.168.0.0/24:

```
!
ip http přístupová třída 75
ip http zabezpečený server
!
přístupový seznam 75 povolení 192.168.0.0 0.0.0.255
přístupový seznam 75 odepřít jakýkoli
!
```

Poznámka : Chcete-li použít přístupový seznam v novějších verzích softwaru Cisco IOS XE, použijte v předchozím příkladu příkaz **ip http access-class ipv4 75 .** Další informace naleznete v části Filtrování provozu určeného pro WebUI zařízení Cisco IOS XE pomocí přístupového seznamu .

I když toto zmírnění bylo nasazeno a osvědčilo se v testovacím prostředí, zákazníci by měli určit použitelnost a efektivitu ve svém vlastním prostředí a za vlastních podmínek použití. Zákazníci by si měli být vědomi toho, že jakékoli implementované řešení nebo zmírnění může negativně ovlivnit funkčnost nebo výkon jejich sítě na základě vlastních scénářů nasazení a omezení zákazníků. Zákazníci by neměli nasazovat žádná náhradní řešení nebo zmírnění dříve, než nejprve vyhodnotí použitelnost pro jejich vlastní prostředí a jakýkoli dopad na takové prostředí.

Opravený software

Společnost Cisco vydala bezplatné aktualizace softwaru , které řeší zranitelnosti popsané v tomto informačním bulletinu. Zákazníci se servisními smlouvami, které je opravňují k pravidelným aktualizacím softwaru, by měli získat opravy zabezpečení prostřednictvím svých obvyklých aktualizačních kanálů.

Zákazníci mohou nainstalovat a očekávat podporu pouze pro verze softwaru a sady funkcí, pro které si zakoupili licenci. Instalací, stažením, přístupem nebo jiným použitím takových aktualizací softwaru zákazníci souhlasí s tím, že budou dodržovat podmínky licence na software Cisco: https://www.cisco.com/c/en/us/products/end-user-license- dohoda.html

Kromě toho mohou zákazníci stahovat pouze software, pro který mají platnou licenci, zakoupený přímo od společnosti Cisco nebo prostřednictvím autorizovaného prodejce nebo partnera společnosti Cisco. Ve většině případů se bude jednat o údržbu upgrade softwaru, který byl zakoupen dříve. Bezplatné aktualizace bezpečnostního softwaru neopravňují zákazníky k získání nové softwarové licence, doplňkových sad funkcí softwaru nebo větších aktualizací revizí.

Stránka Cisco Support and Downloads na Cisco.com poskytuje informace o licencování a stahování. Tato stránka může také zobrazit pokrytí zákaznické podpory zařízení pro zákazníky, kteří používají nástroj Moje zařízení.

Při zvažování upgradů softwaru se zákazníkům doporučuje, aby pravidelně konzultovali doporučení pro produkty Cisco, která jsou k dispozici na stránce Cisco Security Advisories , aby zjistili riziko a kompletní řešení upgradu.

Ve všech případech by se zákazníci měli ujistit, že zařízení, která mají být upgradována, mají dostatek paměti a potvrdit, že aktuální konfigurace hardwaru a softwaru budou v nové verzi i nadále správně podporovány. Pokud informace nejsou jasné, doporučujeme zákazníkům kontaktovat středisko technické pomoci Cisco (TAC) nebo jejich smluvní poskytovatele údržby.

Zákazníci bez servisních smluv

Zákazníci, kteří nakupují přímo od společnosti Cisco, ale nemají smlouvu o poskytování služeb společnosti Cisco, a zákazníci, kteří nakupují prostřednictvím dodavatelů třetích stran, ale nepodařilo se jim získat pevný software prostřednictvím svého prodejního místa, by měli získat upgrady kontaktováním Cisco TAC: https://www . .cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Zákazníci by měli mít k dispozici sériové číslo produktu a být připraveni poskytnout adresu URL tohoto upozornění jako důkaz nároku na bezplatný upgrade.

Opravené verze

Zákazníkům se doporučuje upgradovat na příslušnou pevnou verzi softwaru , jak je uvedeno v následující tabulce:

Cisco IOS XE Software Release Train	První pevná verze	Dostupný
17.9	17.9.4a	Ano
17.6	17.6.6a	TBD
17.3	17.3.8a	TBD
16.12 (pouze katalyzátor 3650 a 3850)	16.12.10a	TBD

Podrobné informace o vydání platformy najdete v tématu Dostupnost opravy softwaru pro chybu zabezpečení eskalace oprávnění webového uživatelského rozhraní softwaru Cisco IOS XE – CVE-2023-20198 .

Tým Cisco Product Security Incident Response Team (PSIRT) ověřuje pouze dotčené a opravené informace o vydání, které jsou zdokumentovány v tomto informačním zpravodaji.

Doporučení

Společnost Cisco důrazně doporučuje zákazníkům, aby deaktivovali funkci HTTP Server na všech systémech s přístupem k internetu nebo omezili jeho přístup na důvěryhodné zdrojové adresy. Chcete-li zakázat funkci HTTP Server, použijte příkaz **no ip http server** nebo **no ip http secure-server** v režimu globální konfigurace. Pokud se používá server HTTP i server HTTPS, jsou k deaktivaci funkce HTTP Server vyžadovány oba příkazy.

Následující rozhodovací strom lze použít k určení způsobu třídění prostředí a nasazení ochran:

Používáte IOS XE?
- **Ne** _ Systém není zranitelný. Není nutná žádná další akce.
- **Ano** _ Je nakonfigurován **ip http server** nebo **ip http secure-server** ?
  - **Ne** _ Zranitelnosti nejsou zneužitelné. Není nutná žádná další akce.
  - **Ano** _ Provozujete služby, které vyžadují komunikaci HTTP/HTTPS (například eWLC)?
    - **Ne** _ Zakažte funkci HTTP Server.
    - **Ano** _ Pokud je to možné, omezte přístup k těmto službám na důvěryhodné sítě.

S velkou jistotou, na základě dalšího pochopení exploitu, hodnotíme, že přístupové seznamy aplikované na funkci HTTP Server k omezení přístupu z nedůvěryhodných hostitelů a sítí představují účinné zmírnění.

Při implementaci řízení přístupu k těmto službám podle poskytnutých zmírnění nezapomeňte zkontrolovat kontroly, protože existuje potenciál pro přerušení produkčních služeb. Pokud si těmito kroky nejste jisti, ve spolupráci s vaší podpůrnou organizací určete vhodná kontrolní opatření.

Po implementaci jakýchkoli změn použijte příkaz **copy running-configuration startup-configuration** k uložení **running-configuration** . To zajistí, že změny nebudou vráceny v případě opětovného načtení systému.

Využití a veřejná oznámení

Společnost Cisco si je vědoma aktivního využívání těchto zranitelností.

Zdroj

Tyto chyby zabezpečení byly nalezeny během řešení několika případů podpory Cisco TAC.

URL

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

Historie revizí

Verze	Popis	Sekce	Postavení	datum
2,0	Aktualizovaný souhrn, který označuje, že je k dispozici vylepšená detekce. Aktualizované indikátory kompromisu s rozšířeným příkazem detekce.	Shrnutí, indikátory kompromisu	Prozatímní	23. října 2023
1.4	Aktualizováno shrnutí, aby bylo uvedeno, že jsou k dispozici první opravy. Přidány konkrétní informace o pevném vydání.	Shrnutí, Opravený software	Prozatímní	22. října 2023

Zobrazit kompletní historii...

Právní vyloučení odpovědnosti

TENTO DOKUMENT JE POSKYTOVÁN „TAK, JAK JE“, A NEIMPLIKUJE ŽÁDNÝ DRUH ZÁRUKY NEBO ZÁRUKY, VČETNĚ ZÁRUK PRODEJNOSTI NEBO VHODNOSTI PRO KONKRÉTNÍ POUŽITÍ. POUŽÍVÁNÍ INFORMACÍ V DOKUMENTU NEBO MATERIÁLŮM Z DOKUMENTU ODKAZOVANÝCH JE NA VLASTNÍ RIZIKO. CISCO SI VYHRAZUJE PRÁVO KDYKOLI ZMĚNIT NEBO AKTUALIZOVAT TENTO DOKUMENT. CISCO OČEKÁVÁ, ŽE TENTO DOKUMENT AKTUALIZUJE, jakmile BUDE K DISPOZICI NOVÉ INFORMACE.

Samostatná kopie nebo parafráze textu tohoto dokumentu, která vynechává distribuční URL, je nekontrolovaná kopie a může postrádat důležité informace nebo obsahovat faktické chyby. Informace v tomto dokumentu jsou určeny koncovým uživatelům produktů Cisco.