TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Az Ivanti VPN termékeket érintő 0. napi kritikus sérülékenységek aktív kihasználásáról

(2024. január 17.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) frissített[1] riasztást ad ki, az **Ivanti Connect Secure** és az **Ivanti Policy Secure** szoftvereket érintő **0. napi, kritikus kockázati** besorolású sérülékenységek kihasználását célzó kibertámadások okán.

A sérülékenységek (**CVE-2023-46805**, **CVE-2024-21887**) az összes támogatott Ivanti Connect Secure (korábbi nevén: Pulse Connect Secure) verziót – **9.x és 22.x** – érintik. A biztonsági rések együttes kihasználása jelentős kiberbiztonsági kockázatot jelent, lehetővé teheti a támadók számára, hogy a hitelesítést megkerülve távolról kódot futtassanak, ami az érintett rendszer **teljes kompromittáláshoz** vezethet.

Figyelmeztetés aktív kihasználásról

A sérülékenységet az amerikai Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökség (CISA) jelzése és kiberbiztonsági piaci szereplők figyelmeztetései alapján **UNC5221** (Mandiant) **UTA0178** (Volexity) azonosítókon jegyzett fenyegetési szereplők ─ vélelmezhetően kiberkémkedési céllal ─ a sérülékenységet célzó támadásokat indítottak (lásd: Indikátorok rész).

Javasolt védelmi intézkedések

A hivatalos hibajavítás megjelenéséig (ami a január 22-ei héten esedékes) a gyártó megkerülő megoldásokat tett közzé. A sérülékenységben érintett ügyfelek számára javasoljuk ezek alkalmazását:

1. Javasolt megismerni a gyártói biztonsági tájékoztatót[2] felvenni a kapcsolatot a gyártói supporttal.
2. A gyártó a sebezhetőség biztonsági kockázatának csökkentése érdekében átmeneti megoldásként javasolja a **mitigation.release.20240107.1.xml** fájl importálását. A fájl alkalmazása néhány funkciót befolyásolhat, ezek a gyártó tájékoztatása szerint a következők:

   - **Ivanti Connect Secure:**

     Admin REST API-k

     - A konfigurációhoz és felügyelethez használt REST API automatizálás érintett. A rendszergazdák a GW GUI felületén keresztül férhetnek hozzá a gateway-ekhez.

     End User Portal (Advanced HTML5)

     - Ez csak azokra a kérésekre vonatkozik, amelyek dinamikusan hozzárendelt HTML5-könyvjelzőt indítanak, a meglévő, előre definiált HTML5-könyvjelzőket ez nem érinti.

A végfelhasználói JSAM funkciót befolyásolja.

Az átíró funkció nem érhető el, ha a kárenyhítést alkalmazták.

- Ez a Rewriter Browser Barra vonatkozik.

A Citrix StoreFront HTML5 érintett

- A CTS/WSAM-on keresztül csatlakozó ICA klienssel rendelkező Citrix Storefront nem érintett.

A PSAL telepítés automatikus elindítása

- Ez csak az új felhasználókra vagy olyan gépekre van hatással, amelyek korábban nem jelentkeztek be, és nem telepítették a PSAL-t. Megoldásként töltse le és telepítse manuálisan a PSAL-t!

Admin CRL konfiguráció

- A rendszergazdák nem tudják módosítani a CRL konfigurációt. A CRL funkciót nem befolyásolja a kockázatcsökkentés.

- **Ivanti Policy Secure:**

  Profiler és Remote Profiler működését jelentős mértékben befolyásolja, ha a kárenyhítést alkalmazzák, de továbbra is lehetővé teszi az IPS-berendezésen történő hitelesítést.

  Az UEBA adaptív hitelesítés nem érhető el, ha a kárenyhítést alkalmazzák.

3. **A gyártói integritásellenőrző eszköz** alkalmazása. A beépített változaton kívül az Ivanti rendelkezik az Integrity Checker Tool továbbfejlesztett változatával, amelyet a szervezetek letölthetnek és az ICS VPN-eken futtathatnak.

   Az Integrity Checker Tool futtatása újraindítja az ICS VPN készüléket, ami azt eredményezi, hogy a rendszermemória tartalma nagyrészt felülíródik. Amennyiben **az eszköz futtatása előtt vannak kompromittálódásra utaló jelek, ajánlott az eszközt nem futtatni, amíg a memória és más bizonyítékok összegyűjtésére sorra nem került.**

   A helyi mentést követően az eszköz futtatása egy csomagnak a kiszolgálóra történő feltöltésével és Service Pack-ként történő telepítésével történik. Az eszköz ezután lefut, és megjeleníti az eredményeit a képernyőn. Ez magában foglalja azt is, hogy felfedezett-e új vagy nem megfelelő fájlokat.

   Miután az ICS VPN készülék újraindul, a váratlan fájlok titkosított pillanatfelvétele elmentésre kerül és letölthető. Ezt a fájlt az Ivanti rendelkezésére lehet bocsátani a visszafejtéshez, és az azonosított váratlan fájlok archivált másolatát tartalmazza.

   Az eszközzel kapcsolatos további részletek, a letöltés és a telepítés módja a KB44755 dokumentumban található.

Kompromittálásra utaló indikátorok (IoC-k):

Az alábbiakban a Volexity által azonosított kulcsfontosságú fájlok listája az alábbi táblázatban található.

Fájlnév	Leírás	Mi célt szolgál7
/home/perl/DSLogConfig.pm	Modified Perl module	Designed to execute **sessionserver.pl**
/home/etc/sql/dsserver/sessionserver.pl	Perl script to remount the filesystem with read/write access	Make **sessionserver.sh** executable, execute it, then restore original mount settings
/home/etc/sql/dsserver/sessionserver.sh	Script executed by **sessionserver.pl**	Uses regular expressions to modify **compcheckresult.cgi** to insert a webshell into it; also creates a series of entries into files associated with the In-build Integrity Checker Tool to evade detection when periodic scans are run
/home/webserver/htdocs/dana-na/auth/compcheckresult.cgi	Modified legitimate component of the ICS VPN appliance, with new Perl module imports added and a one-liner to execute commands based on request parameters	Allows remote code execution over the Internet if the attacker can craft a requests with the correct parameters
/home/webserver/htdocs/dana-na/auth/lastauthserverused.js	Modified legitimate JavaScript component loaded by user login page of the Web SSL VPN component of ICS	Modified to harvest entered credentials and send them to a remote URL on an attacker-controlled domain

Fontos, hogy az ICS VPN-t üzemeltető szervezetek felülvizsgálják a hálózati naplóikat, a hálózati telemetriát és az Integrity Checker Tool (múltbeli és jelenlegi) eredményeit, a sikeres kompromittálódás jeleinek megtalálása érdekében.

Érték	Típus	Leírás
206.189.208[.]156	ipaddress	DigitalOcean IP address tied to UTA0178
gpoaccess[.]com	hostname	Suspected UTA0178 domain discovered via domain registration patterns
webb-institute[.]com	hostname	Suspected UTA0178 domain discovered via domain registration patterns
symantke[.]com	hostname	UTA0178 domain used to collect credentials from compromised devices
75.145.243[.]85	ipaddress	UTA0178 IP address observed interacting with compromised device
47.207.9[.]89	ipaddress	UTA0178 IP address observed

		interacting with compromised device tied to Cyberoam proxy network
98.160.48[.]170	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
173.220.106[.]166	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
73.128.178[.]221	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.243.177[.]161	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.213.208[.]89	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
64.24.179[.]210	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
75.145.224[.]109	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.215.39[.]49	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
71.127.149[.]194	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
173.53.43[.]7	ipaddress	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network

Kiberbiztonsági jelzések alapján **öt egyedi malware** vált ismertté, amelyeket a támadások során a fenyegetési szereplők telepítettek a hosszútávú hozzáférés fenntartásához, további rosszindulatú payloadok telepítéséhez és hitelesítő adatok ellopásához.

A Volexity és a Mandiant által eddig azonosított támadásokban használt eszközök listája:

Zipline passzív backdoor	(file név: libsecure.so.1) egyedi rosszindulatú szoftver, amely képes a hálózati forgalom elfogására, támogatja a feltöltési/letöltési műveleteket, reverse shell-eket, proxy-kiszolgálókat, szerver-tunneleket hoz létre.
Wirefire web shell	(file név: visits.py) Python-alapú egyedi web shell, amely támogatja a nem hitelesített tetszőleges parancsok végrehajtását és a payload telepítését.
Lightwire web shell	(file név: compcheckresult.cgi) Perl nyelven írt, legitim fájlba ágyazott egyedi web shell, amely lehetővé teszi a tetszőleges parancsok végrehajtását.
Warpwire harvester	(file név: lastauthserverused.js) Egyedi JavaScript-alapú eszköz a bejelentkezéskor a hitelesítő adatok begyűjtésére, majd elküldésére egy parancs- és vezérlőkiszolgálónak (C2).

PySoxy tunneler	Megkönnyíti a hálózati forgalom tunnelt a lopakodás érdekében.
BusyBox	Többször hívható bináris program, amely számos, különböző rendszerfeladatokhoz használt Unix segédprogramot egyesít.
Thinspool Dropper	Egyéni shell script dropper, amely a Lightwire webes shell-t írja az Ivanti CS-re, biztosítva a perzisztenciát.
Thinspool utility	(file név: sessionserver.sh)**:** A fájlrendszer "read/write"-ként való újbóli csatlakoztatására szolgál a rosszindulatú programok telepítésének lehetővé tétele érdekében.

A kapcsolódó indikátorok a Volexity GitHub oldaláról is letölthetők:

YARA szabályok

Indikátorok

Hivatkozások:

[1] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-ivanti-termekeket-erinto-0-napi-kritikus-serulekenysegekrol/

[2] https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

[3] https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

[4] https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

- https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways
- https://forums.ivanti.com/s/article/KB44755?language=en_US
- https://github.com/volexity/threat-intel/blob/main/2024/2024-01-10%20Ivanti%20Connect%20Secure/indicators/iocs.csv
- https://github.com/volexity/threat-intel/blob/main/2024/2024-01-10%20Ivanti%20Connect%20Secure/indicators/yara.yar

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu