



ПРИМЕР ОТ ПРАКТИКАТА

От мрежов достъп до компрометиране на Active Directory

Производство (IT и ОТ) · Вътрешен мрежови тест за проникване (с предполагаем достъп до мрежата)

2 критични — многослоен план за укрепване на защитата

Анонимизиран съгласно NDA. Клиентът и идентифициращите детайли са премахнати. PXLSecurity LTD. · София, България · pxlsec.com



ПРИМЕР ОТ ПРАКТИКАТА

От мрежов достъп до компрометиране на Active Directory

Сектор	Производство (ИТ и ОТ)
Ангажимент	Вътрешен мрежови тест за проникване (с предполагаем достъп до мрежата)
Резултат	2 критични — многослоен план за укрепване на защитата

10 хоста, достъпни чрез препредадено удостоверяване	СТОТИЦИ анонимно изброени потребители	НЯКОЛКО открити системи без поддръжка и ОТ системи
---	--	--

ПРЕДИЗВИКАТЕЛСТВОТО

Производител искаше да установи докъде може да достигне нападател с начален мрежов достъп. В слабо сегментираната мрежа съжителстваха съвременна Windows AD среда, системи от среден клас без поддръжка и устройства за оперативни технологии (ОТ).

КАК СЕ РАЗВИ

1. Подменихме отговори при разрешаване на имена чрез LLMNR, NBT-NS и mDNS. Прихванахме и идентификационни данни в открит вид от стара услуга с HTTP Basic удостоверяване.
2. Подписването на SMB беше изключено на множество хостове. Доказахме NTLM relay: чрез препредаване на удостоверяването на машинен акаунт получихме достъп до около десет хоста.
3. Контролерите на домейна не изискваха подписване на LDAP и обвързване на канала. Чрез препредаване на удостоверяването към LDAP извлякохме пълна информация от директорията.
4. Чрез анонимна нулева сесия получихме списък със стотици домейнови потребители и политиката за пароли. Установихме и прекомерно членство в привилегирани групи.
5. Описахме рисковете от системите без поддръжка и ОТ устройствата: четене на файлове през AJP без удостоверяване, протоколи без шифроване и SMBv1 на стара операционна система от среден клас, както и уязвима серия ОТ контролери.

ОСНОВНИ КОНСТАТАЦИИ

Critical	NTLM relay към LDAP (подписването и обвързването на канала не се налагат)
Critical	Неуверено четене на файлове през AJP на сървър без поддръжка
High	Изключено подписване на SMB — препредаване между хостове
High	Анонимно изброяване на AD и прекомерно членство в администраторски групи
High	ОС от среден клас без поддръжка с протоколи в чист текст и SMBv1

ВЪЗДЕЙСТВИЕ

Достъпът до мрежата без потребителски акаунт позволяваше верига от атаки към пълно компрометиране на Active Directory. Устройства за оперативни технологии също бяха достъпни от тази мрежа.

РЕЗУЛТАТ

Предадохме план с няколко нива на защита: подходящи мерки срещу NTLM relay при SMB и LDAP, изключване на LLMNR и NBT-NS, ограничаване на членството в привилегировани групи, извеждане от употреба на системите без поддръжка и сегментация между IT и OT. Планиран беше отделен период за тестване на делегирането и AD CS.

ТЕХНИКИ

NTLM relay · Отравяне на LLMNR/NBT-NS · Подписване на LDAP · Системи без поддръжка · Експозиция на OT

УСЛУГИ

Active Directory и вътрешна мрежа · Тестване за проникване

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, изпълнявани от старши инженери, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331