



ПРИМЕР ОТ ПРАКТИКАТА

Добре защитен периметър — и доказателствата за това

Транспорт и логистика · Външен мрежови тест за проникване (черна кутия,
~80 хоста)

Няма доказани критични или високи уязвимости в проверения обхват

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



ПРИМЕР ОТ ПРАКТИКАТА

Добре защитен периметър — и доказателствата за това

Сектор	Транспорт и логистика
Ангажимент	Външен мрежови тест за проникване (черна кутия, ~80 хоста)
Резултат	Няма доказани критични или високи уязвимости в проверения обхват

~80	0	7+
тествани публични хоста	доказани критични или високи уязвимости	водещи CVE, доказано неексплоатируеми

ПРЕДИЗВИКАТЕЛСТВОТО

Логистична компания искаше да провери голяма интернет среда за известни уязвимости (CVE) с високо въздействие. Изискването беше да се докладват само проблеми с доказан начин за експлоатация, вместо предположения въз основа на обявените версии.

КАК СЕ РАЗВИ

1. Идентифицирахме около осемдесет публични хоста в определения период за тестване.
2. Проверихме всеки приложим CVE с високо въздействие: отдалечено изпълнение на код в пощенски сървър, изтичане на съдържание от паметта на гранични шлюзове и уязвимости в устройства и портали. Проверихме също идентификационни данни по подразбиране и публично достъпни услуги.
3. Потвърдихме, че проверените CVE са отстранени или неексплоатируеми. Шлюзът не разкриваше съдържание от паметта, пътят към отдалечено изпълнение на код не беше достъпен, а типът на съдържанието и Content Security Policy блокираха експлоатацията на отразения вход.
4. Потвърдихме реалните проблеми: публично достъпен обработчик за трасиране, анонимен FTP достъп до празен дял и липсващи SPF и DMARC.
5. Един мрежови блок филтрираше адреса на тестера на приложно ниво. Отбелязахме необходимостта адресът да бъде разрешен и този блок да бъде тестван повторно.

ОСНОВНИ КОНСТАТАЦИИ

Medium	Публично достъпен обработчик за трасиране в ASP.NET, разкриващ данни за заявки и сесии
Low	Анонимен FTP достъп до празен дял
Low	Липсват SPF и DMARC — възможно изпращане на имейли от името на домейна
Positive	Проверените значими CVE са доказано отстранени или неексплоатируеми

ВЪЗДЕЙСТВИЕ

Периметърът беше добре защитен. Потвърденият остатъчен риск се ограничаваше до разкриване на информация и подправяне на подателя на имейл.

РЕЗУЛТАТ

С тестове потвърдихме, че проверените значими CVE са отстранени или не могат да бъдат експлоатирани в тази среда. Предадохме кратък списък с корекции за доказаните проблеми и план за повторно тестване на мрежовия блок, който филтрираше достъпа на тестера. Положителните резултати също бяха подкрепени с доказателства.

ТЕХНИКИ

Докладване само на доказани проблеми · Валидиране на CVE · Картографиране на атакуваната повърхност · Подправяне на имейл (SPF/DMARC)

УСЛУГИ

Тестване за проникване · Оценка на уязвимостите

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