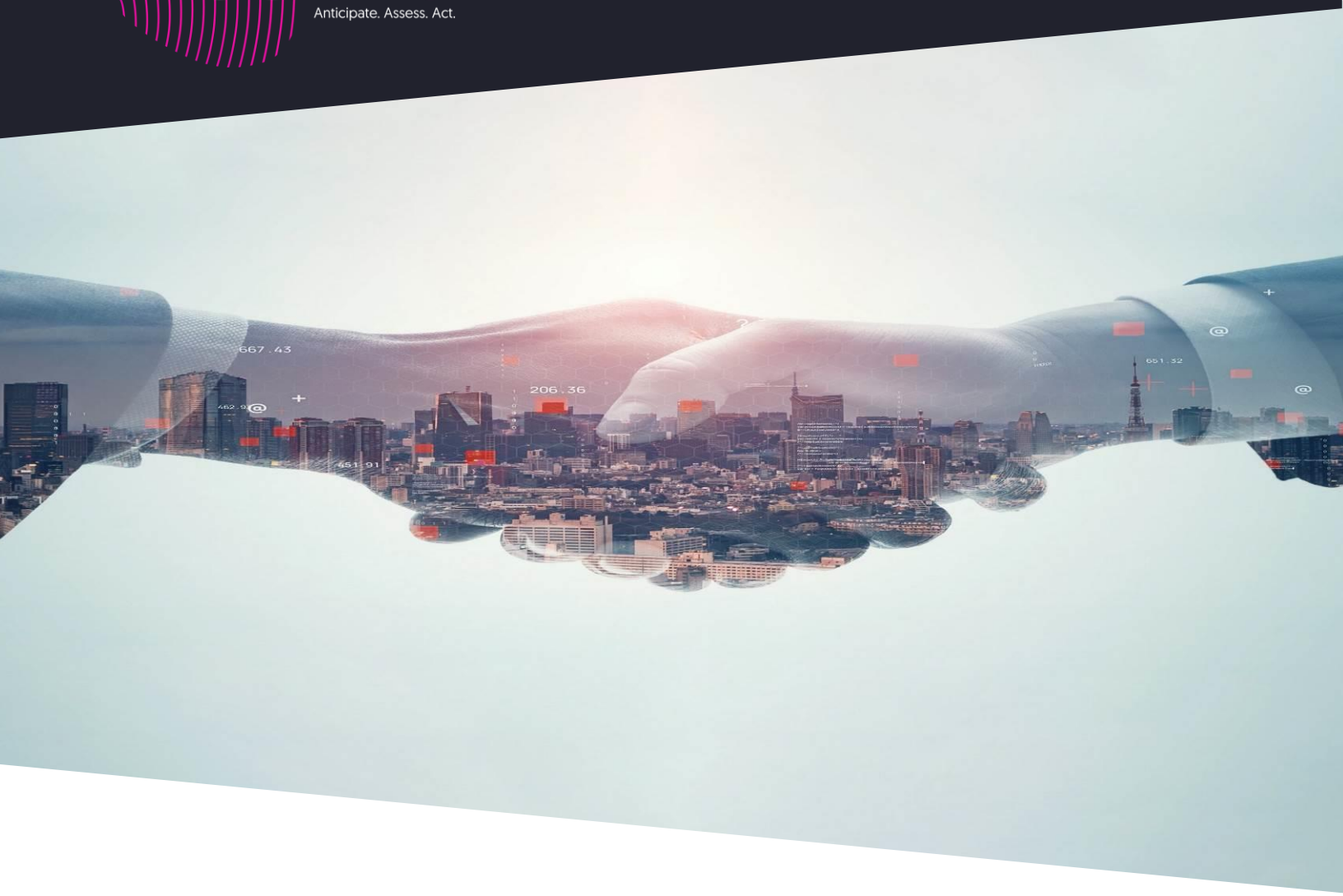
BUGSEC
Anticipate. Assess. Act.



API тест на проникнення

PROVISION ISR

ТОВ "Бугсек" | вул. Нім, 2, Ришон-ле-Ціон, 7546354 | Ізраїль | www.bugsec.com

Деталі проведення

КОРОТКИЙ ВИКЛАД ОБСЯГУ ДОСЛІДЖЕННЯ

Часові рамки проведення	04/06/2024 - 09/06/2024
Оцінка середовища	Продукція
Статус звіту	Заключний
Автори	Аміт Макс
Затверджено	
Версія звіту	1.1
Останнє оновлення	16 червня 2024 року

КОМАНДА З ТЕСТУ НА ПРОНИКНЕННЯ

Технічний керівник проекту	Ошрат Менаше
Виконавець тесту на проникнення	Аміт Макс

ЗАЦІКАВЛЕНІ АКЦІОНЕРИ

ТЕХНІЧНИЙ ДИРЕКТОР	Тал Ханок

Технологічні деталі

Загальний опис

Надана колекція API (набір запитів, що має назву "Загальні запити" всередині колекції) містила запити, що використовуються в основній платформі Provision-ISR, яка дозволяє кінцевому користувачеві взаємодіяти зі встановленими камерами спостереження.
Крім того, було проведено сканування інфраструктури на наступних системах:

Перелік систем, що перевіряються

Назва пристрою	Адреса
Камера та відеореєстратор (Кінцеві точки збору API - 29 запитів)	109.67.159.241 & 109.67.159.239

Обмеження тесту

- API колекція містить 29 запитів, які реалізовані у веб-інтерфейсі камери Provision-ISR.

Вміст тесту

Назва тесту	Статус	ID
Тестування трафіку між клієнтом і сервером	Неуспішно	F1, F3
Спроба впровадження шкідливого коду та обхід валідації. (SQLI, XSS і т.д.)	Успішно	
Керування користувачами та ідентифікація з додатком.	Неуспішно	F2
Тестування можливості захоплення сервера/бази даних.	Успішно	
Витік конфіденційної інформації	Успішно	
Тестування типів апаратного забезпечення сервера/додатків	Успішно	
Витік технічної інформації	Успішно	
Спроба знищити дані / завантажити файли	Успішно	
Обхід бізнес-логіки	Успішно	
Відмова в обслуговуванні / втручання в роботу програми	Успішно	
Тестування механізму управління сесіями в додатку	Успішно	
Виявлення мережевих з'єднань	Успішно	

Детальна інформація

ID	Тема	Загальне пояснення	Рівень ризику
	API тест на проникнення		
1	**F1 – Використання HTTP дозволено**	Було виявлено, що додаток дозволяє доступ через захищений канал HTTPS (HTTP over TLS). Однак перевірка безпеки показала, що сервер також підтримує HTTP-канал	Середній
2	**F2 - Використання базової автентифікації**	Огляд показав, що API підтримує базову автентифікацію	Низький
3	**F3 - HTTP Strict Transport Security налаштовано не повністю**	Під час перевірки було виявлено, що веб-сервер включає заголовок «Strict-Transport-Security» без атрибуту «preload». Крім того, значення атрибуту «max-age» не відповідає найкращим практикам	Інформативний

Результати - API тесту на проникнення

F1 - Використання HTTP дозволено

Загальний рівень ризику: Середній

Ймовірність використання: Середня | Потенційний вплив: Високий

Опис уразливості

Безпека на транспортному рівні (TLS), раніше відома як SSL, шифрує трафік між клієнтом і сервером, щоб запобігти підслуховуванню зловмисниками з'єднання та доступу до конфіденційних даних або їх зміні. Тому правильна конфігурація має вирішальне значення.

Було помічено, що додаток дозволяє доступ через захищений канал HTTPS (HTTP over TLS). Однак перевірка безпеки показала, що сервер також підтримує HTTP-канал.

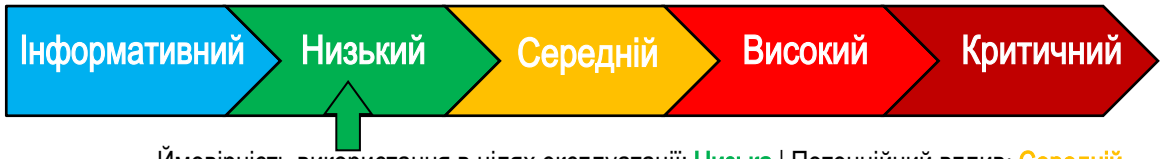
Деталі уразливості

Зловмисники можуть використовувати HTTP для проведення MiTM-атак (Man in the Middle), оскільки трафік програми не шифрується.

Важливо відзначити, що використання HTTP контролюється користувачем, і клієнт може вирішити, чи використовувати HTTP або HTTPS (Provision-ISR рекомендує використовувати HTTPS).

F2 – Використання базової автентифікації

Загальний рівень ризику: Низький



Ймовірність використання в цілях експлуатації: Низька | Потенційний вплив: Середній

Опис уразливості

Базова автентифікація дозволяє веб-браузеру або іншій клієнтській програмі надавати облікові дані (ім'я користувача та пароль) при доступі до програми. Після того, як користувач вводить свої облікові дані, вони об'єднуються, кодуються за допомогою base64 і надсилаються на сервер у заголовку «Авторизація». Хоча кодування base64 робить облікові дані нечитабельними для неозброєного ока, їх можна легко розшифрувати, що робить систему вразливою до атак, пов'язаних з моніторингом трафіку. Тому в безпечних системах слід уникати використання базової автентифікації.

Однак, огляд показав, що API підтримує базову автентифікацію.

Деталі уразливості

Базова автентифікація вважається слабким механізмом автентифікації з кількох причин:

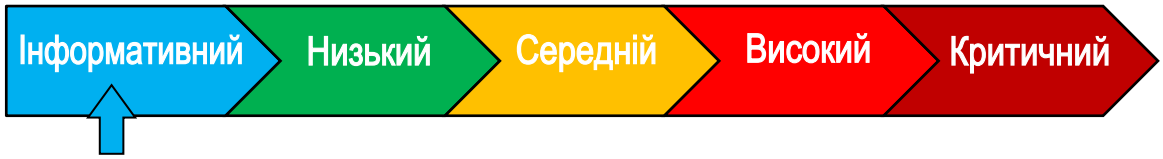
- Реалізація механізму виходу з системи у веб-додатках є більш складною, оскільки додаток не може просто завершити роботу або відкликати облікові дані користувача, на відміну від сеансів або токенів.
- Облікові дані користувача надсилаються з кожним HTTP-запитом між клієнтом і сервером, що підвищує ризик витоку.
- Навіть якщо запити передаються захищеним каналом (SSL/TLS) і вважаються безпечними, канал все одно можна розшифрувати за допомогою різних атак на SSL. Тому бажано не покладатися виключно на SSL/TLS для забезпечення безпеки.
- Це підвищує ймовірність того, що облікові дані користувача зберігаються в різних механізмах кешування і ведення журналів.

Зверніть увагу, що API підтримує зв'язок через HTTP (незашифрований), тому зловмисник, який може здійснити MiTM-атаку, може перехопити відкриті текстові облікові дані.

Крім того, важливо зазначити, що інтерфейс Provision-ISR дозволяє автентифікацію на основі токенів на додаток до базової автентифікації, і клієнт сам вирішує, який метод автентифікації слід увімкнути.

F3 – HTTP Суворий захист передачі даних налаштовано не повністю

Загальний рівень ризику: Інформативний



Ймовірність використання: Інформативна | Потенційний вплив: Інформативний

Опис уразливості

HTTP Strict Transport Security (HSTS) - це механізм безпеки, який веб-додатки вказують у заголовку відповіді. Коли браузер отримує цей заголовок, він гарантує, що весь зв'язок із зазначеним доменом надсилається за протоколом HTTPS, а не HTTP. HSTS також не дозволяє зловмисникам використовувати недійсні сертифікати для перехоплення зв'язку і не дає користувачам обходити попередження про узгодження SSL.

Під час перевірки було виявлено, що веб-сервер включає заголовок «Strict-Transport-Security» без атрибуту «preload». Крім того, значення атрибуту «max-age» не відповідає найкращим практикам.

Деталі уразливості

Зловмисники можуть скористатися початковим запитом на перенаправлення з HTTP на HTTPS, коли браузер ще не закешував домен, і здійснити успішну атаку MiTM (Man in the Middle).

Слід зазначити, що оскільки система встановлена в мережах клієнтів (іноді в закритих мережах), Provision-ISR не може повністю впровадити політику HSTS, тому цей висновок був представлений для інформування зацікавлених сторін і був оцінений як інформативний.

ДОДАТОК А: Визначення ризику вразливості та його критерії

Рейтинг ризику, присвоєний кожній вразливості, визначається шляхом усереднення декількох аспектів використання та середовища, включаючи репутацію, складність та критичність.

Критичний	Критичні вразливості становлять серйозну загрозу безпеці організації і повинні бути негайно усунені. Вони можуть призвести до повної компрометації цільового середовища або подібних критичних наслідків.
Високий	Вразливості з високим рівнем ризику становлять серйозну загрозу для середовища компанії і повинні бути негайно виправлені. Ці проблеми можуть суттєво вплинути на стан безпеки організації.
Середній	Вразливості середнього рівня представляють помірний ризик для середовища. Вони можуть потребувати додаткового контексту перед усуненням, але повинні бути усунені після критичних та високих ризиків.
Низький	Вразливості з низьким рівнем небезпеки створюють мінімальний ризик для цільового середовища і часто є теоретичними за своєю природою. Усунення низьких ризиків часто є менш пріоритетним, ніж інші методи зміцнення безпеки.
Інформативний	Самі по собі інформаційні вразливості мають незначний вплив на цільову сферу або взагалі не впливають на неї. Однак вони включені, оскільки можуть становити ризик у поєднанні з іншими обставинами або технологіями, які наразі відсутні. Виправлення інформаційних вразливостей не є обов'язковим.

ДОДАТОК B: Інструментарій Bugsec

Bugsec використовує комерційне програмне забезпечення та інструменти для аналізу вразливостей і слабких місць у системі безпеки. Ці інструменти постійно розвиваються та змінюються. Щоб бути в курсі технологічних та галузевих тенденцій, Bugsec постійно оновлює та інтегрує нові інструменти, методи та унікальні знання.

Ось основні інструменти, якими користуються наші фахівці під час тестування на проникнення:

- Nmap
- Nessus
- Postman
- BurpSuite
- SSLScan
- Dirbuster
- Nikto