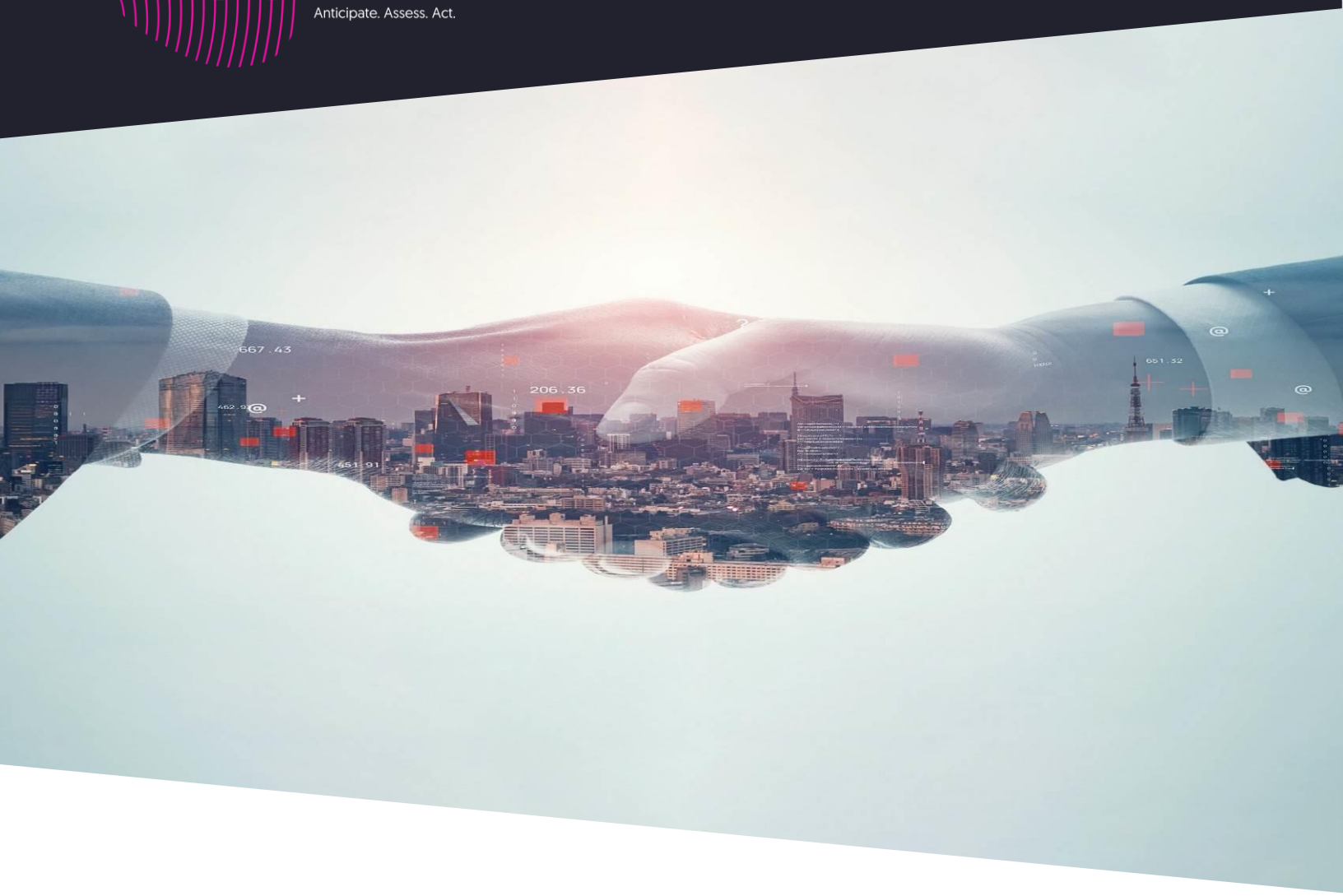
BUGSEC
Anticipate. Assess. Act.



API тест на проникнення та сканування інфраструктури

PROVISION ISR

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

Зміст

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	Виберіть пункт.
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

Процес і методологія

Bugsec використовує складні методи зловмисників високого класу, надаючи унікальну інформацію про ризики та вразливості, які більшість автоматизованих інструментів часто не помічають. Наша широка методологія тестування на проникнення складається з таких етапів:

Розпізнавання

Цей етап починається зі збору інформації та попереднього дослідження досліджуваного середовища. Процес включає в себе використання автоматизованих інструментів і ручних методів, що забезпечує основу для проведення індивідуального тесту на проникнення.

Сканування

Після того, як ціль повністю визначена, Bugsec використовує інструменти сканування вразливостей та ручний аналіз для виявлення недоліків у системі безпеки. Завдяки більш ніж десятирічному досвіду та спеціально розробленим інструментам, наші інженери безпеки знаходять слабкі місця, які більшість автоматизованих сканерів не помічають.

Обробка даних та наступні заходи

На цьому етапі оцінки наші експерти переглядають усі попередні дані, щоб виявити та безпечно використати виявлені вразливості. Після отримання конфіденційного доступу основна увага приділяється ескалації та переміщенню, щоб визначити технічні ризики та загальний вплив на бізнес.

Звітування

Після завершення роботи Bugsec надає детальний звіт про виявлені вразливості та загрози, включаючи кроки з їх усунення. Наш звіт включає виявлені вразливості, які можуть дозволити зловмиснику отримати підвищений рівень доступу або втрутитися в нормальну роботу системи, а також пріоритезацію вразливостей за рівнем ризику.

Виправлення

На додаток до формальної оцінки, Bugsec проводить повторне тестування вразливостей у звіті. Після виправлення вразливостей та отримання запиту від клієнта, Bugsec оновлює звіт з визначенням нового рівня ризику та зазначає, які вразливості у звіті були виправлені, що підтверджує новий рівень ризику.

Короткий зміст

Передумови

Протягом червня 2024 року Bugsec провів API тест на проникнення та тест на сканування інфраструктури для ProvisionISR. Цей тест був проведений для оцінки захисних можливостей ProvisionISR та надання допомоги з безпеки шляхом проактивного виявлення вразливостей, оцінки їхньої серйозності та надання кроків для їх усунення.

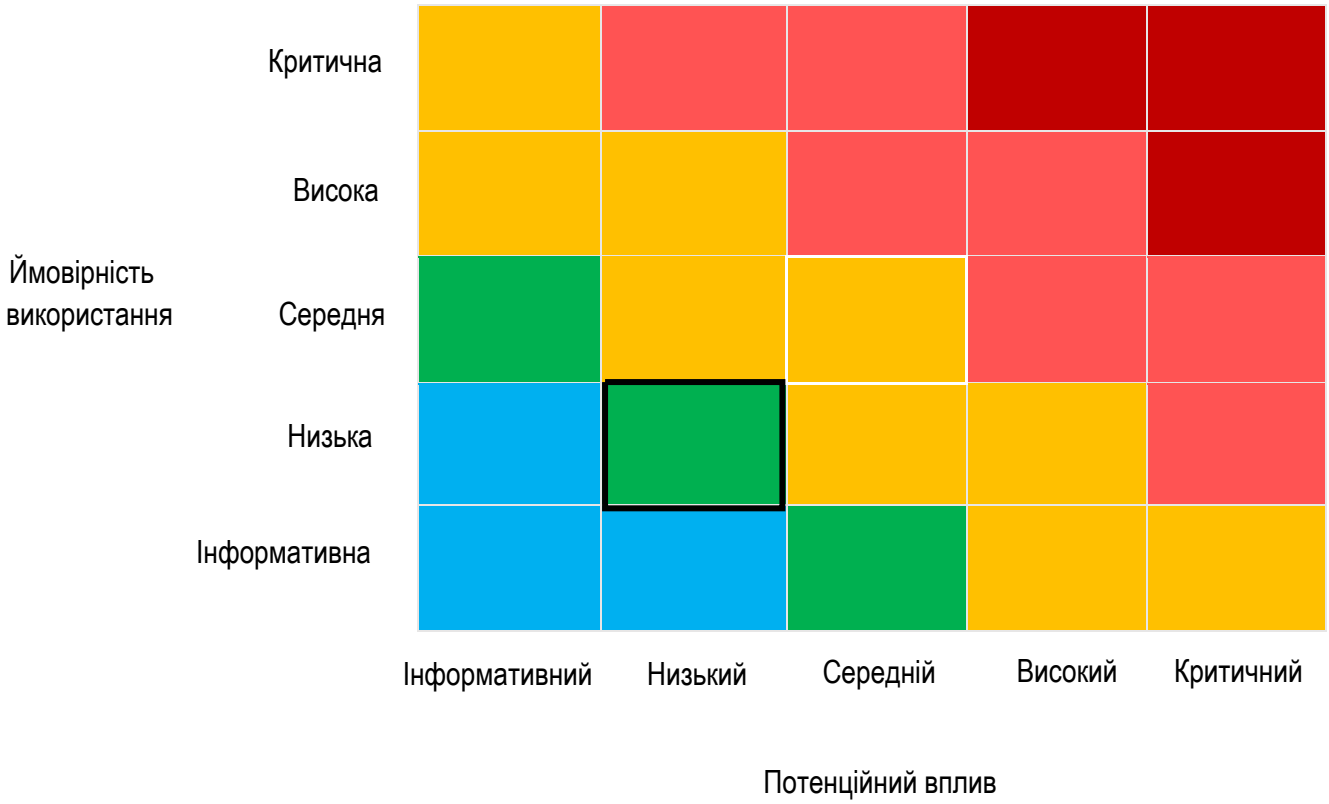
Bugsec перевірив безпеку додатків ProvisionISR і визначив низький ризик компрометації з боку зовнішніх зловмисників, про що свідчить наявність уразливостей, детально описаних у цьому звіті.

Детальні висновки та рекомендації щодо усунення недоліків цих оцінок можна знайти далі у звіті.

Загальний рейтинг ризику - API тест на проникнення

Bugsec розраховує ризик API на основі ймовірності використання (простота експлуатації) та потенційного впливу (потенційний вплив бізнесу на навколишнє середовище).

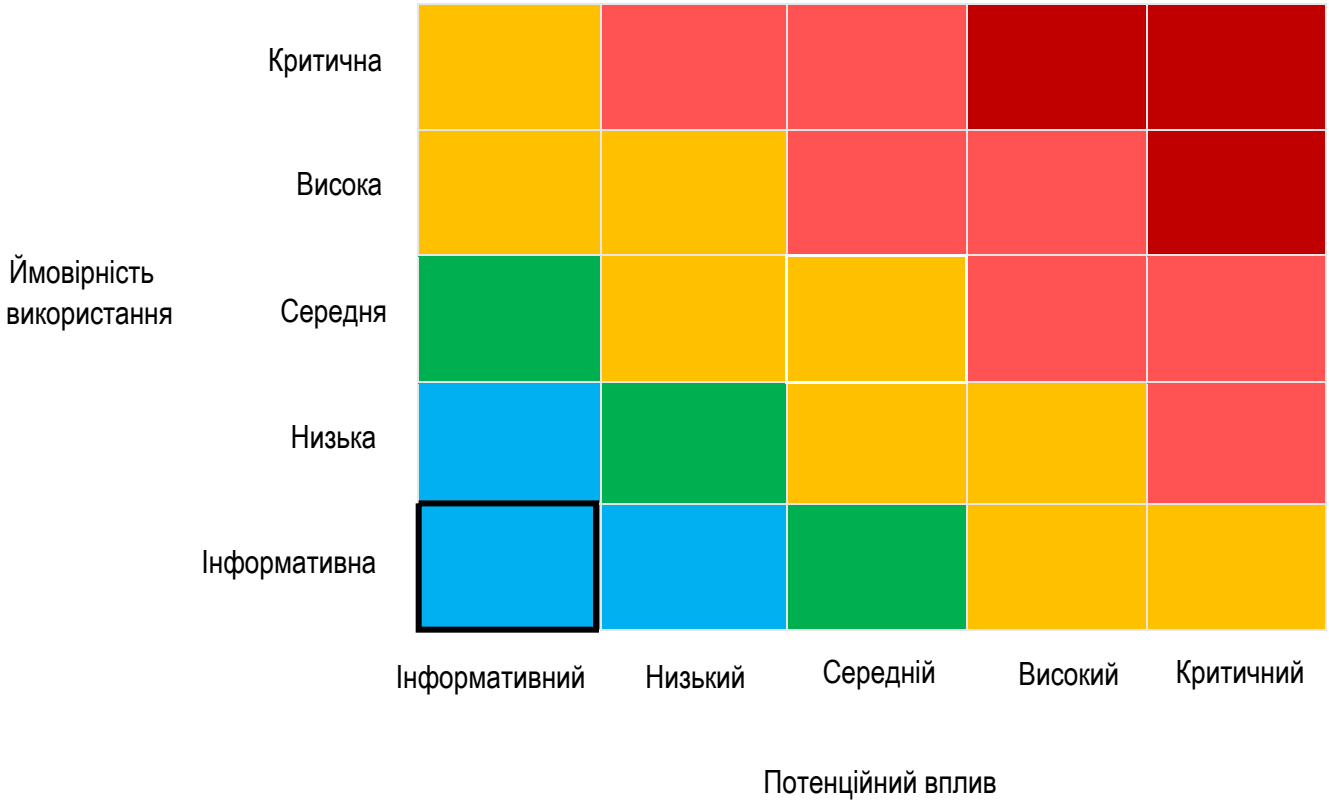
ЗАГАЛЬНИЙ РЕЙТИНГ РИЗИКУ: **Низький**



Загальний рейтинг ризику - тест на перевірку інфраструктури

Bugsec розраховує API ризик на основі ймовірності використання (простота експлуатації) та потенційного впливу (потенційний вплив бізнесу на навколишнє середовище).

ЗАГАЛЬНИЙ РЕЙТИНГ РИЗИКУ: Інформативний



Огляд результатів

Огляд слабких сторін

Bugsec виявив та дослідив уразливості під час оцінювання ProvisionISR. Ми класифікували ці вразливості як загальні слабкі місця в поточному середовищі та надали вказівки щодо їх усунення для підвищення рівня безпеки підприємства.

1. Перевірка безпеки показала, що сервер підтримує канал HTTP.
2. Було виявлено, що API підтримує базову автентифікацію.
3. 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.
4. Під час тестування було виявлено, що деякі бібліотеки на стороні клієнта є застарілими.

Стратегічні рекомендації

Не всі слабкі місця в системі безпеки є технічними і персонал служби безпеки не може усунути їх усі. Компаніям часто доводиться зосереджуватися на корінних проблемах безпеки і вирішувати їх в основі. Ці стратегічні кроки - це зміни в операційній політиці організації. Bugsec рекомендує наступні стратегічні кроки для покращення безпеки ProvisionISR.

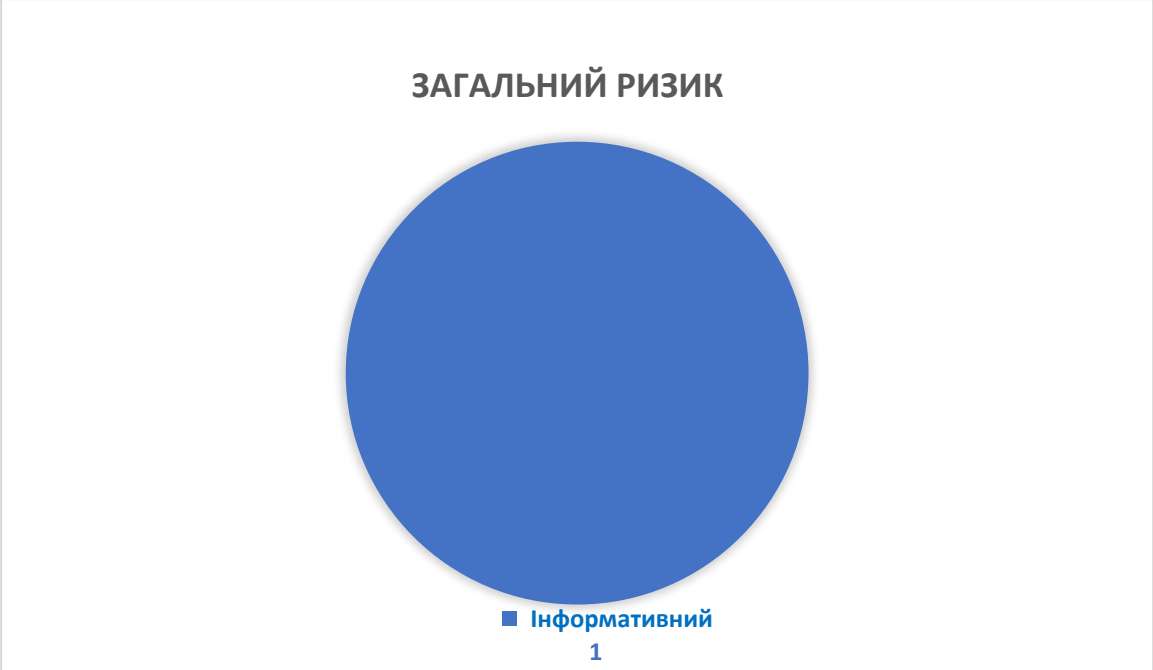
1. Використання HTTP має бути заборонено в додатку. Рекомендується використовувати тільки зашифровані протоколи, такі як HTTPS.
2. Рекомендується використовувати сеансову автентифікацію замість базової автентифікації.
3. Рекомендується налаштувати атрибут «max-age» на 63,072,000 секунд.
4. Рекомендується включити домен компанії до списку попереднього завантаження HSTS. Більше інформації можна знайти за посиланням https://hstspreload.org
5. Рекомендується оновити бібліотеки до останніх версій.

Зведена діаграма вразливостей - API тест на проникнення

На кожному рівні ризику були виявлені наступні вразливості. Важливо знати, що загальна кількість вразливостей не є фактором для визначення рівня ризику. Рівень ризику залежить від серйозності виявлених вразливостей.

Зведена діаграма вразливостей - тест сканування інфраструктури

На кожному рівні ризику були виявлені наступні вразливості. Важливо знати, що загальна кількість вразливостей не є фактором для визначення рівня ризику. Рівень ризику залежить від серйозності виявлених вразливостей.



Технологічні деталі

Загальний опис

Надана колекція API (набір запитів, що має назву "Загальні запити" всередині колекції) містила запити, що використовуються в основній платформі ProvisionISR, 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 ProvisionISR.

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
		Тест на сканування інфраструктури	
4	F1 - Застарілі бібліотеки JavaScript на стороні клієнта	Під час тестування було виявлено, що деякі бібліотеки на стороні клієнта є застарілими	Інформативний

Результати - API тесту на проникнення

F1 - Використання HTTP дозволено

Загальний рівень ризику: Середній

Ймовірність використання: Низька | 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

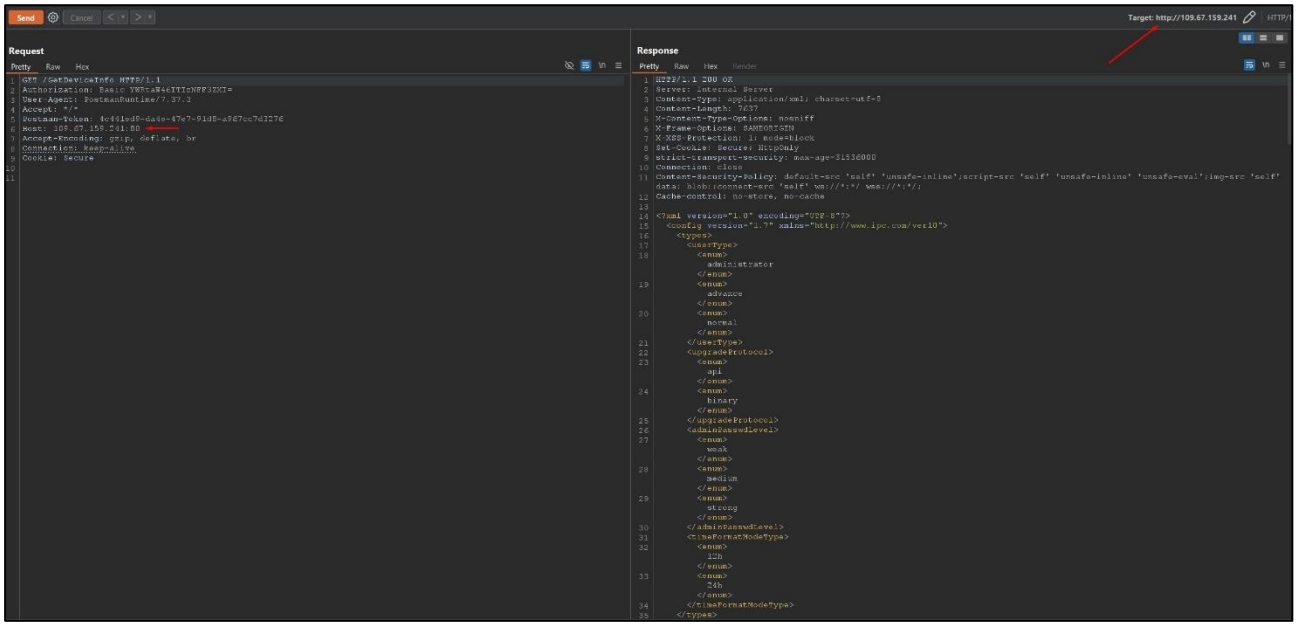
Зловмисники можуть використовувати HTTP для проведення MiTM-атак (Man in the Middle), оскільки трафік програми не шифрується.

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

Скріншоти

На наступному зображенні показано запит, успішно відправлений на сервер по HTTP (незашифрований).

URL: http://109.67.159.241/GetDeviceInfo

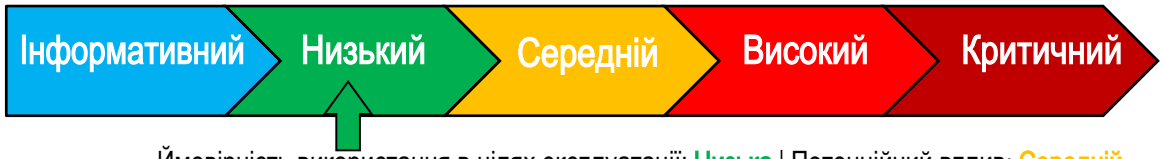


Зменшення ризиків та рекомендації

- Використання HTTP має бути заборонено в додатку. Рекомендується використовувати тільки зашифровані протоколи, такі як 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 ProvisionISR дозволяє автентифікацію на основі токенів на додаток до базової автентифікації, і клієнт сам вирішує, який метод автентифікації слід увімкнути.

Скріншоти

На наступному зображенні показано одну з кінцевих точок API колекції API, яка підтримує базову автентифікацію.

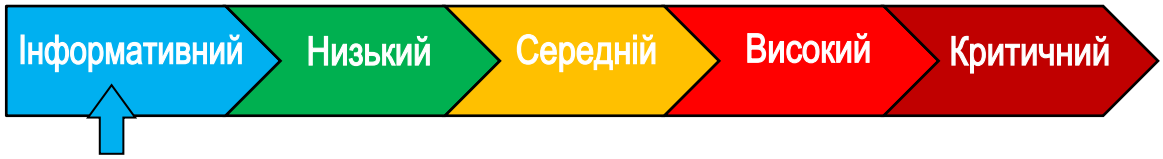
URL: http://109.67.159.241/SetNetBasicConfig

Зниження ризиків та рекомендації

- Рекомендується використовувати сеансову автентифікацію замість базової автентифікації.

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

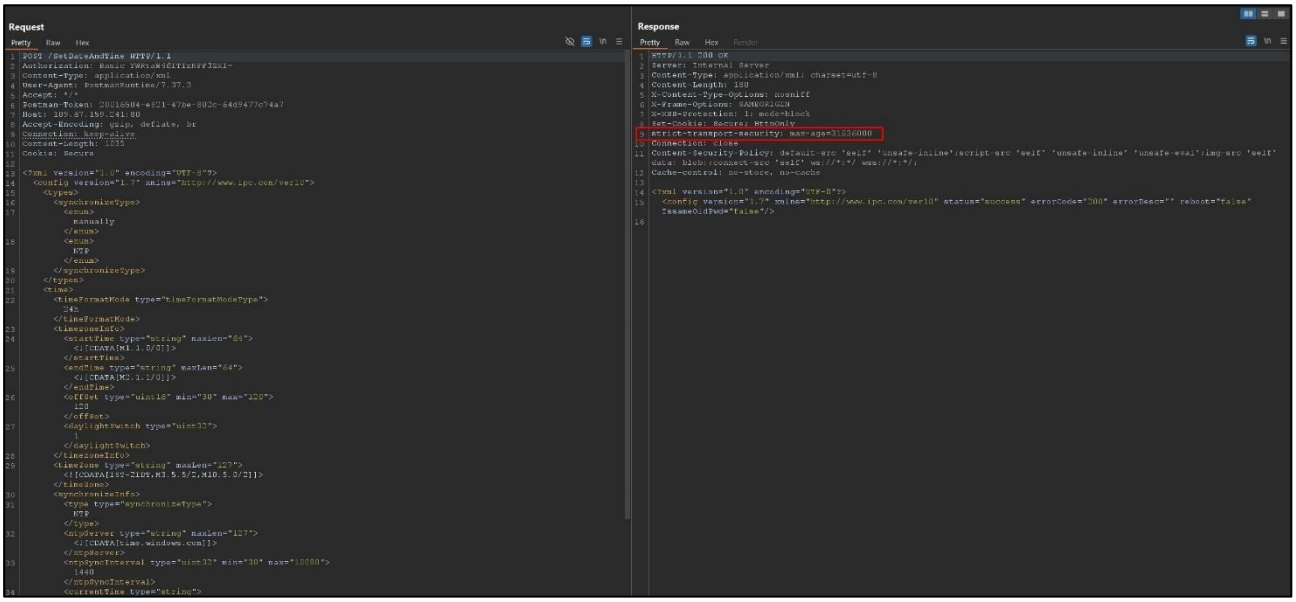
Зловмисники можуть скористатися початковим запитом на перенаправлення з HTTP на HTTPS, коли браузер ще не закешував домен, і здійснити успішну атаку MiTM (Man in the Middle).

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

Скріншоти

На наступному зображенні показано, що заголовок HSTS не містить атрибута 'preload'. Крім того, атрибут 'max-age' має значення 31,536,000 секунд замість 63,072,000 секунд.

URL: http://109.67.159.241/SetDateAndTime



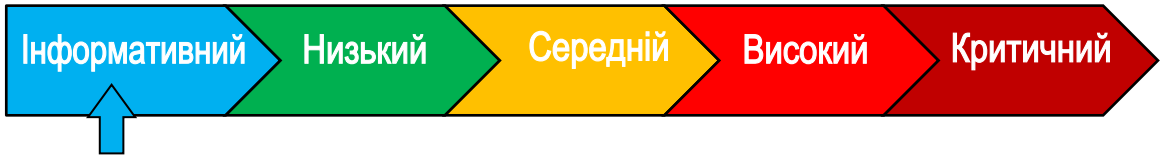
Зниження ризиків та рекомендації

- Рекомендується налаштувати атрибут "max-age" на 63,072,000 секунд.
- Рекомендується включити домен компанії до списку попереднього завантаження HSTS. Більше інформації можна знайти на сайті https://hstspreload.org.

Результати - Тест сканування інфраструктури

F1 – Застарілі бібліотеки JavaScript на стороні клієнта

Загальний рівень ризику: Інформативний



Ймовірність використання: Інформативна | Потенційний вплив: Інформативний

Опис уразливості

Оновлення безпеки - це виправлення, які усувають недоліки та відсутні елементи керування в програмному забезпеченні, призначені для усунення вразливостей. Отже, постійне оновлення програмного забезпечення та сервісів є одним з найважливіших аспектів забезпечення безпеки.

Під час тестування було виявлено, що деякі бібліотеки на стороні клієнта є застарілими.

Деталі уразливості

Відсутність оновлень програмного забезпечення та формального або автоматизованого процесу виправлення помилок безпеки робить додаток вразливим до відомих атак. Залежно від характеру вразливості, відсутність оновлень може зробити додаток вразливим до атак на відмову в обслуговуванні або дозволити зловмисникам отримати доступ до інформації з обмеженим доступом.

Зверніть увагу, що цей результат оцінюється як інформативний, оскільки для застарілих версій не було виявлено жодних серйозних вразливостей, і він був піднятий лише для інформування відповідного персоналу.

Скріншоти

Наступні зображення демонструють використання застарілих клієнтських бібліотек JavaScript, що використовуються обома серверами: **IP:** 109.67.159.241

IP: 109.67.159.239

Зниження ризиків та рекомендації

- Рекомендується оновити бібліотеки до останніх версій.

ДОДАТОК А: Зміни в деталях середовища

Наступні зміни були внесені в середовище в рамках проекту. Вони не обов'язково представляють значний вплив на середовище, але включені для повного обліку модифікацій командою тестування на проникнення в Bugsec Ltd.

БЕЗ ЗМІН

Не було внесено жодних змін до середовища, таких як створення нових облікових записів користувачів або завантаження файлів до цільової системи. Це надається в якості повного обліку модифікацій командою тестування на проникнення в Bugsec Ltd.

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

ДОДАТОК C: 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.

About Bugsec

BugSec пропонує комплексні рішення з кібербезпеки для глобальних підприємств, надаючи їм життєво важливі інструменти для проактивного виявлення, оцінки та протидії кіберзагрозам. Оскільки компанії переходять на хмарні технології, наша передова платформа CDR, CYCL, створює надійну та безпечну основу для ваших операцій з безпеки - ідеальне поєднання технологій та експертизи.

Наша місія в BugSec полягає в тому, щоб надавати масштабовані керовані продукти та рішення для виявлення та реагування на загрози, захищаючи критичні дані та системи організацій як у публічних, так і в приватних хмарних середовищах. Ми прагнемо надавати індивідуальні рішення, адаптовані до унікальних потреб кожної організації, за підтримки нашої команди досвідчених професіоналів з кібербезпеки для ефективного реагування на інциденти безпеки та зменшення ризиків.

Послуги Bugsec

✓ CYCL Платформа

CYCL пропонує оптимізовані, прозорі та хмаро орієнтовані операції з безпеки для бізнесу, що знаходиться в русі. Завдяки нашим послугам керованого хмарного виявлення та реагування (CDR), пристосованим як для мультихмарних, так і для локальних установок, ми пропонуємо економічно ефективне та адаптивне рішення для сучасних кіберзагроз.

✓ IR (Реагування на інциденти)

BugSec IRT поєднує в собі досвід, гнучкість та непохитну прихильність до захисту вашого бізнесу від кіберзагроз. Незалежно від того, коли стався інцидент, ми готові втрутитися, ефективно нейтралізувати загрози та швидко відновити ваші бізнес-операції.

Наші фахівці IRT знаходяться в режимі 24/7, щоб швидко виявляти, аналізувати та пом'якшувати наслідки інцидентів, пов'язаних з безпекою. Від виявлення першопричини до впровадження надійних стратегій виправлення - ми готові мінімізувати час простою та захистити критичні активи вашої організації.

✓ Червона команда

Залучаючи нашу Червону команду для проведення наступальних операцій, ви отримаєте уявлення про надійність системи безпеки вашої організації. В епоху все більш складних і витончених кіберзагроз важливим є багатогранний підхід. Хоча технології відіграють вирішальну роль, наша червона команда підкреслює, що справді надійна стратегія кібербезпеки включає в себе перспективу зловмисника.

Наші досвідчені фахівці ретельно оцінюють ваші організаційні засоби контролю, виявляючи та усуваючи вразливості, які можуть існувати у вашій системі безпеки. Такий проактивний підхід забезпечує підвищену стійкість до потенційних кіберзагроз.

За допомогою наших експертів Red Team ми забезпечуємо вам душевний спокій, який приходить від усвідомлення того, що ваші заходи з кібербезпеки є комплексними та ефективними.

✓ Фіолетова команда

Посильте свій захист від кіберзагроз за допомогою нашого передового сервісу Purple Team Service - динамічного та спільного підходу, який легко інтегрує наступальну тактику червоної команди з оборонними стратегіями синьої команди.

Наша команда експертів організовує імітацію кібератак, щоб ретельно протестувати та посилити систему безпеки вашої організації. Сприяючи співпраці в режимі реального часу між наступальними та захисними командами, ми забезпечуємо комплексну оцінку вашої стійкості до нових загроз, надаючи практичні рекомендації для безпрецедентного пом'якшення наслідків загроз. Удоскональте свою стратегію кібербезпеки за допомогою нашої послуги Purple Team Service - найкращого захисту ваших цифрових активів.

✓ Дослідження

Дослідницька команда Bugsec - це вістря списа, коли справа доходить до найбільш особливих і складних завдань. Наша команда складається з найкращих людських і технологічних ресурсів, які приведуть вас до успіху. Наша команда складається з колишніх військових спеціалістів з найсучасніших наступальних та оборонних підрозділів, групи інженерів з найпрестижніших університетів та багаторічного досвіду роботи в галузі кібербезпеки.

Наша команда здатна проактивно виявляти вразливості за допомогою дослідження апаратного та програмного забезпечення, дослідження вразливостей та аналізу коду, зворотного інжинірингу, аналізу шкідливого програмного забезпечення, надаючи постачальникам та розробникам ретельну документацію для забезпечення надійної безпеки продукту. Співпрацюючи з бізнесом, ми гарантуємо, що навіть незначні зміни в коді залишаються захищеними від потенційних загроз, гарантуючи безпеку ваших програмних рішень.