Adrift Corporation

Company Introduction

2026 Aug 05

Contents

Chapter

I

Company
Information

Chapter

II

Entrepreneur
Introduction

Chapter

III

Services
Introduction

01

Company Information

会社概要

Company Information

Name	Adrift Corporation
Location	Dogenzaka Tokyu bldg. 2F-C, 1-10-8 Dogenzaka, Shibuya, Tokyo, Japan
CEO	Mitsuki Hirota
Business	Cyber security
WEB	https://www.adriftjb.com/
Founded	February 2023
Established	May 2026

02

Entrepreneur Introduction

代表者の紹介

Entrepreneur Introduction

Mitsuki Hirota

Hokkai Gakuen university,
Bachelor of Economics

University of Massachusetts Lowell
MBA enrolled

Registered Information Security Specialist number 023127

Former **police officer** with the Tokyo Metropolitan Police.

After leaving the police force, worked in temporary positions at warehouses and supermarkets before transitioning into the IT industry.
Joined Intersoft Corporation, an India-based IT company, and was stationed in India, where I was responsible for software testing and quality assurance.

Later joined CBRE, a U.S.-based real estate services company, where I led business process automation initiatives and supported financial management for construction projects. While at CBRE, earned the **Registered Information Security Specialist** (RISS) certification and became a freelance cybersecurity engineer.

As a cybersecurity engineer, gained hands-on experience implementing Endpoint Detection and Response (EDR) and operating Security Information and Event Management (SIEM). As a freelance, led the launch of a vulnerability assessment service for the IT subsidiary of a Japanese manufacturing company. Within two years, grew annual revenue from **JPY 5 million to JPY 18 million**, more than tripling the business.

In 2026, established a cybersecurity company while continuing to work as a cybersecurity freelance. Currently focused on **expanding the customer base and growing the business**.

03

Services Introduction

サービスの紹介

Services

WEB Vulnerability Assessment

We provide monthly vulnerability assessments for your web applications using industry-standard security scanners. To provide greater value than automated scanning alone, we also use password lists that reflect techniques commonly used by real-world attackers.

OSINT

We search the Internet for publicly exposed information that could provide attackers with clues about your organization. The results may reveal unexpected exposures that could be leveraged in a cyberattack, enabling you to address potential risks before they become security incidents.

Services

WEB Vulnerability Assessment

Features

Use of scanning tool

We perform vulnerability assessments using industry-standard security scanning tool.
The tool automatically tests for more than 100 types of security vulnerabilities.

Conducted monthly

We perform vulnerability assessment every month. Many organizations conduct vulnerability assessments only once a year. However, new vulnerabilities are discovered every day, making annual assessments insufficient to address today's rapidly evolving threat landscape.

*One-time assessment is not available. A minimum six months subscription is required.

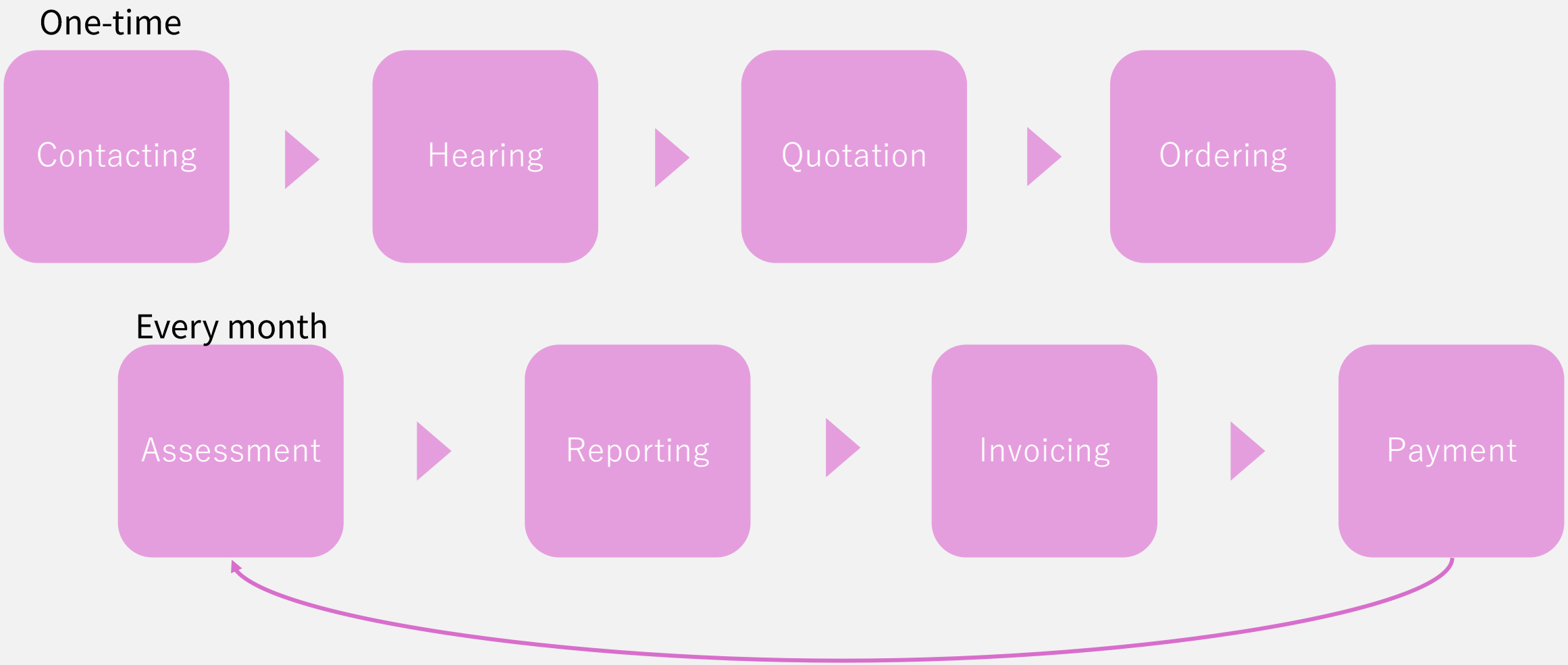
Reliable password list

We use reliable password dictionaries as part of our security assessments.
Since administrator login pages are one of the primary targets of cyberattacks, we conduct focused authentication testing using password lists based on techniques commonly used by real-world attackers.

Services

WEB Vulnerability Assessment

Service flow



WEB Vulnerability Assessment

Price

JPY 100,000 per website / month (excluding tax)

※

- Large-scale websites or test on business logic require a separate quotation.
- A minimum contract period of six months is required.
- Please provide a test account for the vulnerability assessment.

OSINT

Menu

OSINT stands for Open-Source Intelligence.
We investigate publicly available information, primarily from the Internet, to identify information about your organization that could be leveraged by attackers.

Attack surface Management

We identify your publicly exposed domains, subdomains, and open ports to assess your external attack surface.

1 domain
JPY 100,000/month

Passwords and Accounts breach survey

We check whether your email addresses have appeared in known data breaches and identify the types of compromised information.

≦100 e-mail addresses
JPY 50,000
≦ 1,000 e-mail addresses
JPY 300,000

Vulnerability information search

We identify publicly disclosed vulnerabilities based on your software, hardware, and version information.

1 asset
JPY 10,000/month

Document leakage survey

We identify potentially leaked confidential files on the Internet.

1 domain
JPY 100,000/month

Typosquatting survey

We identify domains similar to your organization's domain. (e.g., google.com → goggle.com)

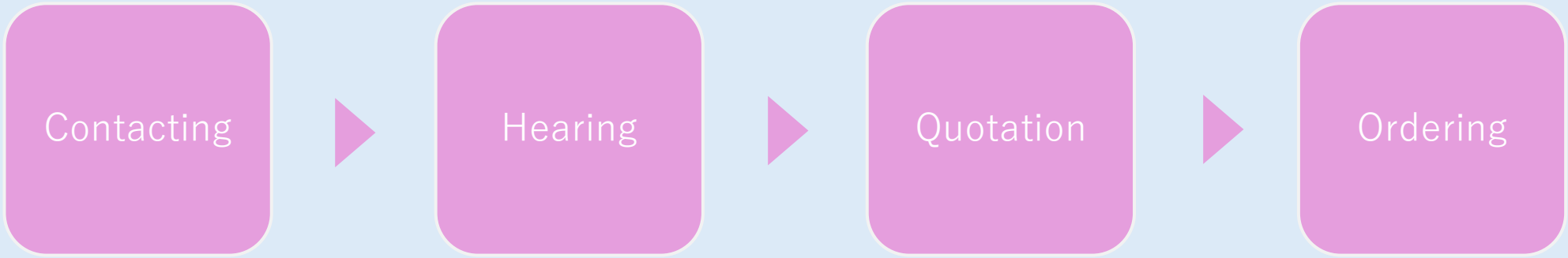
1 domain
JPY 50,000/month

*All prices exclude tax.

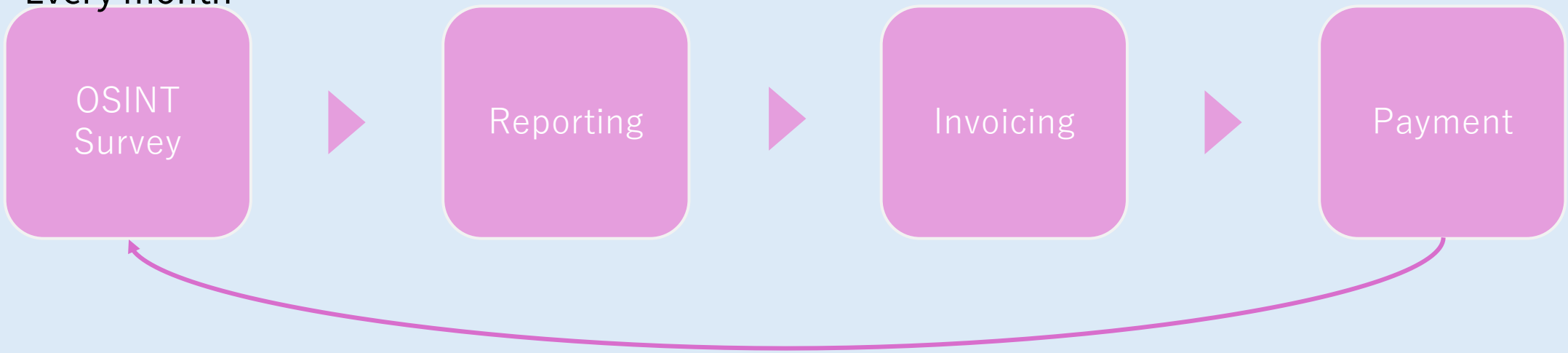
OSINT

Service Flow

One-time



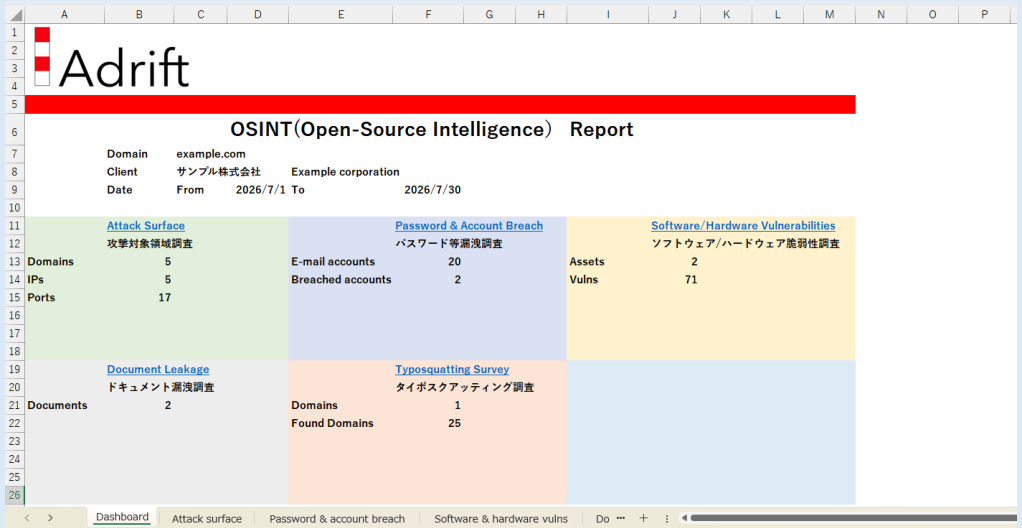
Every month



Services

OSINT

Samples of OSINT Report



Adrift

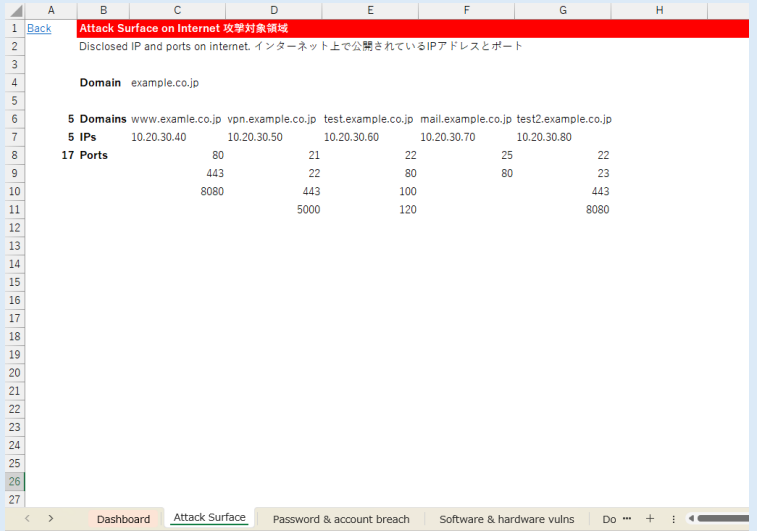
OSINT(Open-Source Intelligence) Report

Domain	example.com		
Client	サンプル株式会社	Example corporation	
Date	From 2026/7/1	To	2026/7/30

Attack Surface 攻撃対象領域調査		Password & Account Breach パスワード等漏洩調査		Software/Hardware Vulnerabilities ソフトウェア/ハードウェア脆弱性調査	
Domains	5	E-mail accounts	20	Assets	2
IPs	5	Breached accounts	2	Vulns	71
Ports	17				

Document Leakage ドキュメント漏洩調査		Typosquatting Survey タイポスクアッティング調査	
Documents	2	Domains	1
		Found Domains	25

Dashboard | Attack surface | Password & account breach | Software & hardware vulns | Do



Back

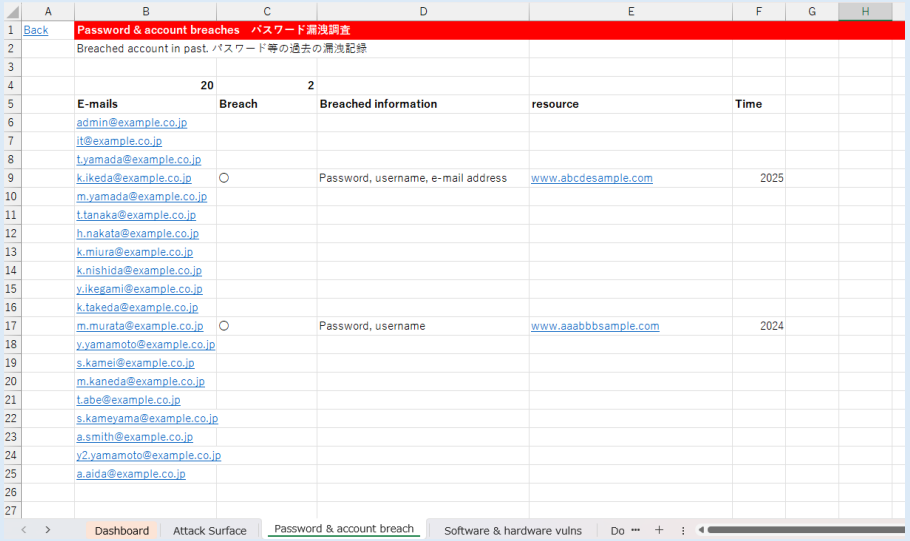
Attack Surface on Internet 攻撃対象領域

Disclosed IP and ports on internet. インターネット上で公開されているIPアドレスとポート

Domain example.co.jp

5 Domains	www.examle.co.jp	vpn.example.co.jp	test.example.co.jp	mail.example.co.jp	test2.example.co.jp	
5 IPs	10.20.30.40	10.20.30.50	10.20.30.60	10.20.30.70	10.20.30.80	
17 Ports	80	21	22	25	22	
	443	22	80	80	23	
	8080	443	100		443	
		5000	120		8080	

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do



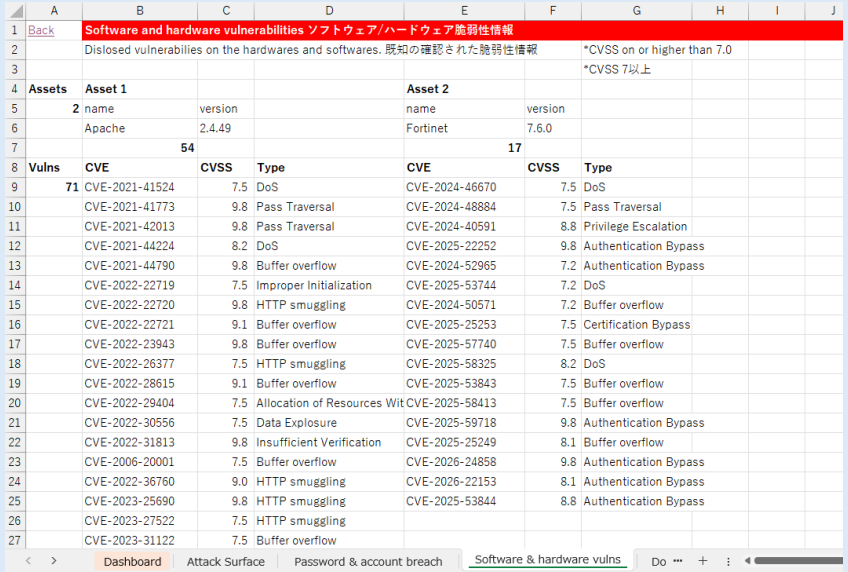
Back

Password & account breaches パスワード漏洩調査

Breached account in past. パスワード等の過去の漏洩記録

20	**2**				
E-mails	**Breach**	**Breached information**	**resource**	**Time**	
admin@example.co.jp					
it@example.co.jp					
t.yamada@example.co.jp					
k.ikeda@example.co.jp	○	Password, username, e-mail address	www.abcdesample.com	2025	
m.yamada@example.co.jp					
t.tanaka@example.co.jp					
h.nakata@example.co.jp					
k.miura@example.co.jp					
k.nishida@example.co.jp					
y.ikegami@example.co.jp					
k.takeda@example.co.jp					
m.murata@example.co.jp	○	Password, username	www.aaabbbsample.com	2024	
y.yamamoto@example.co.jp					
s.kamei@example.co.jp					
m.kaneda@example.co.jp					
t.abe@example.co.jp					
s.kameyama@example.co.jp					
a.smith@example.co.jp					
y2.yamamoto@example.co.jp					
a.aida@example.co.jp					

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do



Back

Software and hardware vulnerabilities ソフトウェア/ハードウェア脆弱性情報

Dislosed vulnerabilies on the hardwares and softwares. 既知の確認された脆弱性情報 *CVSS on or higher than 7.0

*CVSS 7以上

Assets	**Asset 1**			**Asset 2**		
2	name	version		name	version	
	Apache	2.4.49		Fortinet	7.6.0	
	54			**17**		
Vulns	**CVE**	**CVSS**	**Type**	**CVE**	**CVSS**	**Type**
71	CVE-2021-41524	7.5	DoS	CVE-2024-46670	7.5	DoS
	CVE-2021-41773	9.8	Pass Traversal	CVE-2024-48884	7.5	Pass Traversal
	CVE-2021-42013	9.8	Pass Traversal	CVE-2024-40591	8.8	Privilege Escalation
	CVE-2021-44224	8.2	DoS	CVE-2025-22252	9.8	Authentication Bypass
	CVE-2021-44790	9.8	Buffer overflow	CVE-2024-52965	7.2	Authentication Bypass
	CVE-2022-22719	7.5	Improper Initialization	CVE-2025-53744	7.2	DoS
	CVE-2022-22720	9.8	HTTP smuggling	CVE-2024-50571	7.2	Buffer overflow
	CVE-2022-22721	9.1	Buffer overflow	CVE-2025-25253	7.5	Certification Bypass
	CVE-2022-23943	9.8	Buffer overflow	CVE-2025-57740	7.5	Buffer overflow
	CVE-2022-26377	7.5	HTTP smuggling	CVE-2025-58325	8.2	DoS
	CVE-2022-28615	9.1	Buffer overflow	CVE-2025-53843	7.5	Buffer overflow
	CVE-2022-29404	7.5	Allocation of Resources Wit	CVE-2025-58413	7.5	Buffer overflow
	CVE-2022-30556	7.5	Data Explosure	CVE-2025-59718	9.8	Authentication Bypass
	CVE-2022-31813	9.8	Insufficient Verification	CVE-2025-25249	8.1	Buffer overflow
	CVE-2006-20001	7.5	Buffer overflow	CVE-2026-24858	9.8	Authentication Bypass
	CVE-2022-36760	9.0	HTTP smuggling	CVE-2026-22153	8.1	Authentication Bypass
	CVE-2023-25690	9.8	HTTP smuggling	CVE-2025-53844	8.8	Authentication Bypass
	CVE-2023-27522	7.5	HTTP smuggling			
	CVE-2023-31122	7.5	Buffer overflow			

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do

Contact

E-mail
sales@adrift-jp.com

WEB
https://www.adriftjb.com/
*Top page>Service>OSINT or WEB vulnerability Assessment

*We'll reply to you within about three business days.

Thank you !