株式会社XYZ　御中

アタックサーフェス調査報告書

【xyz-company.co.jp】

202X年〇月〇日
株式会社ソリトンシステムズ

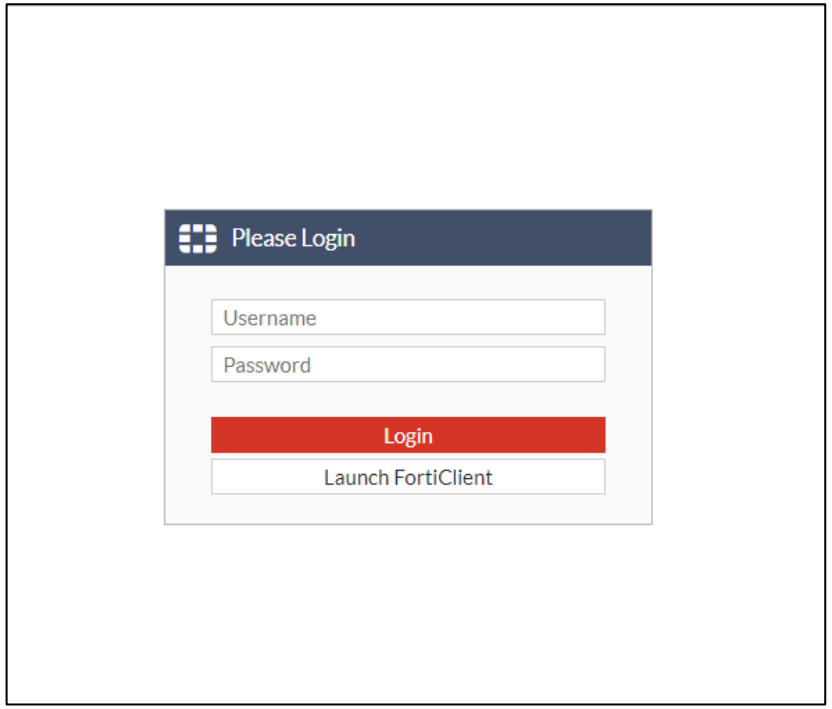
INDEX

第3章　調査結果詳細

3.1. 公開されているWEBログイン画面

調査の結果、下記の認証画面が公開されております。WEBメールの認証画面が公開されています。漏洩アカウントも確認されているので、多要素認証、アクセス元の制限、証明書認証を導入して認証画面を出さないなど、対応を検討される事をお勧めいたします。

IT資産名	IPアドレス	国
vpn.xyz-company.co.jp	x.x.x.x	オランダ



IT資産名	IPアドレス	国
mail.xyz-company.co.jp	x.x.x.x	イタリア

3.2. 公開されているその他のログインプロンプト

SSHリモートアクセスとFTPのログインプロンプトが公開されております。SSHは、アクセスを許可するIPアドレスを制限するか、制限できなければ認証方式をパスワード認証を禁止し、公開鍵認証を利用することをお勧めします。これにより悪意のある第三者にアカウントが漏れても、アカウントだけではログインが出来なくなります。FTPは通信が暗号化されません。認証の通信も平文で行われます。SSHサーバーも動いているようなので、代わりにSCPを使うなどを検討することをお勧めします。

IT資産名	IPアドレス	国	サービス名	プロトコル	ポート番号
www.xyz-company.co.jp	x.x.x.x	アメリカ	SSH	TCP	22

```
$ ssh root@www.xyz-company.co.jp
root@www.xyz-company.co.jp's password:
```

www.xyz-company.co.jp	x.x.x.x	アメリカ	FTP	TCP	21

```
$ ftp www.xyz-company.co.jp
Connected to www.xyz-company.co.jp.
220 FTP on www.xyz-company.co.jp ready
Name (www.xyz-company.co.jp:user1):
```

3.4.漏洩が確認されたメールアドレスとパスワードの状況

■株式会社XYZ

名前の推測	メールアドレス	漏洩事件	ID情報	パスワード情報			その他の漏洩情報や備考・参考情報など
				平文	暗号化	ヒント	
あいず mh	mh.aizu@xyz-company.co.jp	DropBox			●		
あいはら ひろき	hiroki.aihara@xyz-company.co.jp	Adobe	●		●		
あおき しげお	shigeo.aoki@xyz-company.co.jp	AntiPublic		●			
		LastFM		●			
		Myspace	●		●		
あおき ようじ	youji.aoki@xyz-company.co.jp	Adobe	●		●	●	
あおとa	a.aoto@xyz-company.co.jp	Myspace	●		●		
あおやま y	y.aoyama@xyz-company.co.jp	AntiPublic		●			
		ExploitIn		●			
		LinkedIn			●		
あさい ひでお	hideo.asai@xyz-company.co.jp	DropBox			●		
あさお ゆか	yuka.asao@xyz-company.co.jp	Stratfor	●		●		

3.5. ソフトウェア脆弱性

■ 攻撃リスクの高い脆弱性

攻撃が観測されている脆弱性や、リモートから攻撃可能な攻撃コードが公開されている脆弱性があります。
攻撃が観測されている脆弱性
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
攻撃コードが公開されている脆弱性
https://www.exploit-db.com/

下記はサイバー攻撃を受けるリスクの高い脆弱性となりますので、「対策(JVN)」列のリンク先をご確認の上、対策をご検討ください。
これ以外の脆弱性については別添のエクセルファイルをご参照ください。

No.	CVE-ID	CVSS	タイトル	ホスト名	攻撃観測	攻撃コードの公開	対策 (JVN)
1	CVE-2015-1635	10	複数の Microsoft Windows 製品の HTTP.sys における任意のコードを実行される脆弱性	www.xyz-company.co.jp	有	有	リンク
2	CVE-2018-7584	7.5	PHP におけるバッファエラーの脆弱性	www.xyz-service1.jp	無	有	リンク
3	CVE-2019-0211	7.2	Apache HTTP Server における認可・権限・アクセス制御に関する脆弱性	www.xyz-service1.jp	有	有	リンク
4	CVE-2021-40438	6.8	Apache HTTP Server におけるリモートユーザが選択したオリジンサーバにリクエストを転送される脆弱性	www.xyz-service2.jp	有	無	リンク
5	CVE-2014-0160	5	OpenSSL の heartbeat 拡張に情報漏えいの脆弱性	www.xyz-service2.jp	有	有	リンク