Attack Surface
診断レポート

vuln-ruhuna.net

本レポートは、2025年2月20日時点の情報に基づき作成されています。

お問い合わせ先：wa-asm-support@ntt.com
NTTコミュニケーションズ株式会社

目次

1. 診断対象

トップドメイン「vuln-ruhuna.net」を基点として、以下に示すIPアドレスおよびドメイン名を検出しました。本レポートでは、これらのIPアドレスおよびドメイン名に対して、Attack Surfaceに関する診断を実施し、その結果を記載しております。

No	IPアドレス	ドメイン名
1	54.65.19.9	・vuln-ruhuna.net
2	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net
3	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net
4	18.177.168.148	・vulhub.test.vuln-ruhuna.net ・wp.vulhub.test.vuln-ruhuna.net ・webmin.vulhub.test.vuln-ruhuna.net ・zabbix.vulhub.test.vuln-ruhuna.net
5	54.250.173.23	・vulhub.test.vuln-ruhuna.net ・wp.vulhub.test.vuln-ruhuna.net ・webmin.vulhub.test.vuln-ruhuna.net ・zabbix.vulhub.test.vuln-ruhuna.net

2. 診断結果 - 概要

今回の診断結果は下記となります。

緊急	高	中	低	情報
12件	50件	89件	10件	9件

リスクレベル	説明
緊急	攻撃の対象となった場合、被害が甚大、もしくは攻撃が容易に実行可能な状態
高	攻撃の対象となった場合、影響が大きい、またはある程度の知識や技術、推測ができれば攻撃が可能な状態
中	攻撃の対象となった場合、影響が限定的または間接的で、攻撃の実行難易度が比較的高い状態
低	攻撃の対象となった場合、影響が軽微であり、攻撃の実行には複数の条件が必要など、実現が困難な状態
情報	セキュリティ上の潜在的なリスクや改善の余地があるポイントを示す情報

早急に対策が必要な「緊急」の脅威は下記の通りです。

緊急	1. CVE-2024-4577 - phpにおける不正PHPコード実行に関する脆弱性の検出			
攻撃例	・CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1	1
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1	1
緊急	2. CVE-2024-38476 - http_serverにおける情報漏えいに関する脆弱性の検出			
攻撃例				
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	http_server 2.4.58	1
緊急	3. CVE-2024-38474 - http_serverにおけるスクリプト実行に関する脆弱性の検出			
攻撃例	・CWE-116: Improper Encoding or Escaping of Output			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	http_server 2.4.58	1
緊急	4. CVE-2024-11236 - phpにおける整数オーバーフローに関する脆弱性の検出			
攻撃例	・CWE-190: Integer Overflow or Wraparound			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1	1
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1	1
緊急	5. CVE-2023-3824 - phpにおけるメモリ破損またはリモートコード実行に関する脆弱性の検出			
攻撃例	・CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	57.180.175.6	・www.vuln-ruhuna.net	php 8.2.1	1

		・blog.vuln-ruhuna.net		
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1	1
緊急	6. CVE-2022-2068 - openssl における任意コマンド実行に関する脆弱性の検出			
攻撃例	・CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k	1
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k	1
緊急	7. CVE-2022-1292 - openssl におけるコマンドインジェクションに関する脆弱性の検出			
攻撃例	・CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')			
解決方法	インストールされているソフトウェアパッケージをアップグレードしてください。			
対象のIT資産	アセット名	ドメイン名	使用ソフトウェア	件数
1	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k	1
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k	1

3. 診断結果 - 詳細

以下は、危険度が「緊急」「高」「中」「低」「情報」に分類された脅威の一覧です。将来的に重大なリスクに発展する脅威が存在するため、対策を講じることを推奨します。

No	カテゴリ	内容	アセット名	危険度	件数
1	ソフトウェア	CVE-2024-4577 - phpにおける不正PHPコード実行に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	緊急	2
2	ソフトウェア	CVE-2024-38476 - http_serverにおける情報漏えいに関する脆弱性の検出	・54.199.229.228	緊急	1
3	ソフトウェア	CVE-2024-38474 - http_serverにおけるスクリプト実行に関する脆弱性の検出	・54.199.229.228	緊急	1
4	ソフトウェア	CVE-2024-11236 - phpにおける整数オーバーフローに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	緊急	2
5	ソフトウェア	CVE-2023-3824 - phpにおけるメモリ破損またはリモートコード実行に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	緊急	2
6	ソフトウェア	CVE-2022-2068 - opensslにおける任意コマンド実行に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	緊急	2
7	ソフトウェア	CVE-2022-1292 - opensslにおけるコマンドインジェクションに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	緊急	2
8	ソフトウェア	CVE-2024-5585 - phpにおける任意のコマンド実行に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
9	ソフトウェア	CVE-2024-40898 - http_serverにおけるntlmハッシュの流出に関する脆弱性の検出	・54.199.229.228	高	1
10	ソフトウェア	CVE-2024-38477 - http_serverにおけるサーバークラッシュに関する脆弱性の検出	・54.199.229.228	高	1
11	ソフトウェア	CVE-2024-27316 - http_serverにおけるメモリ枯渇に関する脆弱性の検出	・54.199.229.228	高	1
12	ソフトウェア	CVE-2023-3823 - phpにおけるローカルファイル漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
13	ソフトウェア	CVE-2023-0662 - phpにおけるサービス拒否(DoS)に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
14	ソフトウェア	CVE-2023-0568 - phpにおける不正なデータアクセスに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
15	ソフトウェア	CVE-2023-0567 - phpにおける認証バイパスに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
16	ソフトウェア	CVE-2023-0464 - opensslにおけるサービス拒否(DoS)に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
17	ソフトウェア	CVE-2023-0286 - opensslにおけるメモリ漏洩またはDoSに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
18	ソフトウェア	CVE-2023-0215 - opensslにおける解放済みメモリ使用に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
19	ソフトウェア	CVE-2022-0778 - opensslにおけるサービス拒否(DoS)に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
20	ソフトウェア	CVE-2021-3712 - opensslにおけるメモリ情報漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
21	ソフトウェア	CVE-2021-23840 - opensslにおけるアプリケーション誤動作に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
22	ソフトウェア	CVE-2018-0732 - opensslにおけるサービス拒否(DoS)に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
23	ソフトウェア	CVE-2013-4365 - http_serverにおけるバッファオーバーフローに関する脆弱性の検出	・54.199.229.228	高	1
24	ソフトウェア	CVE-2013-2220 - phpにおけるサービス拒否に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	高	2
25	ソフトウェア	CVE-2011-2688 - http_serverにおけるSQL実行に関する脆弱性の検出	・54.199.229.228	高	1
26	ソフトウェア	CVE-2011-1047 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
27	ソフトウェア	CVE-2010-2924 - wordpressにおける任意のSQL実行に関する脆弱性の検出	・54.199.229.228	高	1
28	ソフトウェア	CVE-2010-0673 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
29	ソフトウェア	CVE-2009-4748 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
30	ソフトウェア	CVE-2009-4672 - wordpressにおける任意ファイルの挿入に関する脆弱性の検出	・54.199.229.228	高	1

No	カテゴリ	内容	アセット名	危険度	件数
31	ソフトウェア	CVE-2009-4424 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
32	ソフトウェア	CVE-2009-3703 - wordpressにおける任意のSQL実行に関する脆弱性の検出	・54.199.229.228	高	1
33	ソフトウェア	CVE-2009-2396 - wordpressにおけるリモートコード実行に関する脆弱性の検出	・54.199.229.228	高	1
34	ソフトウェア	CVE-2009-2383 - wordpressにおける任意SQL命令実行に関する脆弱性の検出	・54.199.229.228	高	1
35	ソフトウェア	CVE-2009-2144 - wordpressにおける任意のSQL実行に関する脆弱性の検出	・54.199.229.228	高	1
36	ソフトウェア	CVE-2009-2143 - wordpressにおけるリモートコード実行に関する脆弱性の検出	・54.199.229.228	高	1
37	ソフトウェア	CVE-2009-2122 - wordpressにおけるSQLインジェクション攻撃に関する脆弱性の検出	・54.199.229.228	高	1
38	ソフトウェア	CVE-2009-0968 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
39	ソフトウェア	CVE-2008-7040 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
40	ソフトウェア	CVE-2008-4734 - wordpressにおける不正操作可能に関する脆弱性の検出	・54.199.229.228	高	1
41	ソフトウェア	CVE-2008-4732 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
42	ソフトウェア	CVE-2008-4625 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
43	ソフトウェア	CVE-2008-1982 - wordpressにおけるSQLインジェクションに関する脆弱性の検出	・54.199.229.228	高	1
44	ソフトウェア	CVE-2007-4723 - http_serverにおける認証バイパスに関する脆弱性の検出	・54.199.229.228	高	1
45	ソフトウェア	CVE-2024-5458 - phpにおける誤ったURL解析に関する脆弱性の検出	・54.199.229.228 ・57.180.175.6	中	2
46	ソフトウェア	CVE-2024-2408 - phpにおけるマービン攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
47	ソフトウェア	CVE-2024-11234 - phpにおけるhttpリクエストスマグリングに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
48	ソフトウェア	CVE-2024-11233 - phpにおけるメモリ領域の漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
49	ソフトウェア	CVE-2024-0727 - opensslにおけるサービス拒否攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
50	ソフトウェア	CVE-2023-5678 - opensslにおけるサービス拒否攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
51	ソフトウェア	CVE-2023-3817 - opensslにおけるサービス拒否に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
52	ソフトウェア	CVE-2023-2650 - opensslにおけるサービス拒否に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
53	ソフトウェア	CVE-2023-0466 - opensslにおける無効な証明書に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
54	ソフトウェア	CVE-2023-0465 - opensslにおけるポリシーチェック回避に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
55	ソフトウェア	CVE-2022-4304 - opensslにおけるデータ復号に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
56	ソフトウェア	CVE-2021-4160 - opensslにおけるDH鍵の漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
57	ソフトウェア	CVE-2021-23841 - opensslにおけるサービス拒否に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
58	ソフトウェア	CVE-2020-1971 - opensslにおけるサービス拒否攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
59	ソフトウェア	CVE-2019-1559 - opensslにおけるパディングオラクル攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
60	ソフトウェア	CVE-2019-1551 - opensslにおける難攻不破のRSAまたはDH攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
61	ソフトウェア	CVE-2019-1547 - opensslにおける完全鍵回復に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
62	ソフトウェア	CVE-2018-5407 - opensslにおけるタイミング攻撃悪用に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
63	ソフトウェア	CVE-2018-0739 - opensslにおけるサービス拒否攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
64	ソフトウェア	CVE-2018-0737 - opensslにおける秘密鍵漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
65	ソフトウェア	CVE-2018-0734 - opensslにおける秘密鍵の漏洩に関する脆弱性の検出	・57.180.175.6	中	2

No	カテゴリ	内容	アセット名	危険度	件数
			・54.199.229.228		
66	ソフトウェア	CVE-2017-3738 - openssIにおけるキー情報漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
67	ソフトウェア	CVE-2017-3737 - openssIにおけるデータ漏洩に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
68	ソフトウェア	CVE-2017-3736 - openssIにおけるdh鍵回復に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
69	ソフトウェア	CVE-2017-3735 - openssIにおける証明書表示の誤りに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
70	ソフトウェア	CVE-2013-2765 - http_serverにおけるサービス拒否(DoS)に関する脆弱性の検出	・54.199.229.228	中	1
71	ソフトウェア	CVE-2013-0942 - http_serverにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
72	ソフトウェア	CVE-2012-4360 - http_serverにおけるクロスサイトスクリプティングに関する脆弱性の検出	・54.199.229.228	中	1
73	ソフトウェア	CVE-2012-4001 - http_serverにおける不正なHTTPリクエストに関する脆弱性の検出	・54.199.229.228	中	1
74	ソフトウェア	CVE-2012-3526 - http_serverにおけるサービス拒否(DoS)に関する脆弱性の検出	・54.199.229.228	中	1
75	ソフトウェア	CVE-2011-1176 - http_serverにおける特権の昇格に関する脆弱性の検出	・54.199.229.228	中	1
76	ソフトウェア	CVE-2011-0759 - wordpressにおけるCSRF攻撃に関する脆弱性の検出	・54.199.229.228	中	1
77	ソフトウェア	CVE-2011-0740 - wordpressにおけるクロスサイトスクリプティングに関する脆弱性の検出	・54.199.229.228	中	1
78	ソフトウェア	CVE-2011-0641 - wordpressにおけるクロスサイトスクリプティングに関する脆弱性の検出	・54.199.229.228	中	1
79	ソフトウェア	CVE-2010-4747 - wordpressにおけるスクリプト注入に関する脆弱性の検出	・54.199.229.228	中	1
80	ソフトウェア	CVE-2010-4637 - wordpressにおけるクロスサイトスクリプティングに関する脆弱性の検出	・54.199.229.228	中	1
81	ソフトウェア	CVE-2010-4630 - wordpressにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
82	ソフトウェア	CVE-2010-4518 - wordpressにおける不正スクリプト実行に関する脆弱性の検出	・54.199.229.228	中	1
83	ソフトウェア	CVE-2010-4403 - wordpressにおける情報漏洩に関する脆弱性の検出	・54.199.229.228	中	1
84	ソフトウェア	CVE-2010-4402 - wordpressにおける任意スクリプト注入に関する脆弱性の検出	・54.199.229.228	中	1
85	ソフトウェア	CVE-2010-4277 - wordpressにおける任意スクリプト挿入に関する脆弱性の検出	・54.199.229.228	中	1
86	ソフトウェア	CVE-2010-3977 - wordpressにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
87	ソフトウェア	CVE-2010-1186 - wordpressにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
88	ソフトウェア	CVE-2009-4170 - wordpressにおける情報漏洩に関する脆弱性の検出	・54.199.229.228	中	1
89	ソフトウェア	CVE-2009-4169 - wordpressにおけるスクリプト注入に関する脆弱性の検出	・54.199.229.228	中	1
90	ソフトウェア	CVE-2009-4168 - wordpressにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
91	ソフトウェア	CVE-2009-3767 - openssIにおけるNoneに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
92	ソフトウェア	CVE-2009-3766 - openssIにおけるSSLサーバースプーフィングに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
93	ソフトウェア	CVE-2009-3765 - openssIにおけるSSLなりすましに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
94	ソフトウェア	CVE-2009-2852 - wordpressにおける任意コード実行に関する脆弱性の検出	・54.199.229.228	中	1
95	ソフトウェア	CVE-2009-2299 - http_serverにおけるサービス拒否(DoS)に関する脆弱性の検出	・54.199.229.228	中	1
96	ソフトウェア	CVE-2009-1390 - openssIにおける中間者攻撃に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
97	ソフトウェア	CVE-2008-7175 - wordpressにおけるクロスサイトスクリプティングに関する脆弱性の検出	・54.199.229.228	中	1
98	ソフトウェア	CVE-2008-6811 - wordpressにおける任意コード実行に関する脆弱性の検出	・54.199.229.228	中	1
99	ソフトウェア	CVE-2008-5752 - wordpressにおけるファイル開示に関する脆弱性の検出	・54.199.229.228	中	1
100	ソフトウェア	CVE-2008-4733 - wordpressにおける任意スクリプト注入に関する脆弱性の検出	・54.199.229.228	中	1
101	ソフトウェア	CVE-2007-5800 - wordpressにおけるリモートコード実行に関する脆弱性の検出	・54.199.229.228	中	1
102	ソフトウェア	CVE-2007-3205 - phpにおける任意変数の上書きに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	中	2
103	ソフトウェア	CVE-2007-2627 - wordpressにおけるクロスサイトスクリプトに関する脆弱性の検出	・54.199.229.228	中	1
104	ソフトウェア	CVE-2023-3247 - phpにおけるメモリ情報漏洩に関する脆弱性の検出	・57.180.175.6	低	2

No	カテゴリ	内容	アセット名	危険度	件数
			・54.199.229.228		
105	ソフトウェア	CVE-2020-1968 - openssIにおける盗聴に関する脆弱性の検出	・54.199.229.228 ・57.180.175.6	低	2
106	ソフトウェア	CVE-2019-1563 - openssIにおける暗号鍵の復元に関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	低	2
107	ソフトウェア	CVE-2019-1552 - openssIにおける不正アクセスに関する脆弱性の検出	・57.180.175.6 ・54.199.229.228	低	2
108	ソフトウェア	CVE-2013-0941 - http_serverにおける機密情報漏えいに関する脆弱性の検出	・54.199.229.228	低	1
109	ソフトウェア	CVE-2009-0796 - http_serverにおけるスクリプト注入に関する脆弱性の検出	・54.199.229.228	低	1
110	ネットワーク	WAFの検出	・www.vuln-ruhuna.net	情報	1
111	ネットワーク	TLSバージョンの検出	・www.vuln-ruhuna.net	情報	1
112	ネットワーク	SSL証明書発行者の検出	・www.vuln-ruhuna.net	情報	1
113	ネットワーク	SSL DNS Namesの検出	・www.vuln-ruhuna.net	情報	1
114	ネットワーク	SOAレコードサービスの検出	・www.vuln-ruhuna.net	情報	1
115	ネットワーク	HTTPセキュリティヘッダー欠如の検出	・www.vuln-ruhuna.net	情報	1
116	ネットワーク	DNS SaaSサービスの検出	・www.vuln-ruhuna.net	情報	1
117	ネットワーク	CAAレコードの検出	・www.vuln-ruhuna.net	情報	1
118	ネットワーク	Apacheの検出	・www.vuln-ruhuna.net	情報	1

No1. ソフトウェア

CVE-2024-4577 - phpにおける不正PHPコード実行に関する脆弱性の検出

CVE-2024-4577 - A vulnerability related to unauthorized PHP execution in php is Detected

緊急

2件

説明

PHP バージョン 8.1.* (8.1.29 以前)、8.2.* (8.2.20 以前)、8.3.* (8.3.8 以前) では、Windows 上で Apache と PHP-CGI を使用する場合、 特定のコードページを使用するようにシステムが設定されていると、 Windows が "Best-Fit" 動作を使用して Win32 API 関数に指定されたコマンドラインの文字を置き換えることがあります。PHP CGI モジュールはこれらの文字を PHP のオプションと誤認する可能性があり、 悪意のあるユーザが実行中の PHP バイナリにオプションを渡すことで、 スクリプトのソースコードを公開したり、サーバ上で任意の PHP コードを実行したりすることができます。

解決方法

インストールされているソフトウェアパッケージをアップグレードしてください。

攻撃例

・CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

脆弱なバージョン

8.1.* ~ 8.1.29　8.2.* ~ 8.2.20　8.3.* ~ 8.3.8

参考資料

・https://www.php.net/ChangeLog-8.php#8.1.29
・https://cert.be/en/advisory/warning-php-remote-code-execution-patch-immediately
・https://security.netapp.com/advisory/ntap-20240621-0008/
・https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html
・https://www.php.net/ChangeLog-8.php#8.2.20

対象のIT資産

No	アセット名	ドメイン名	使用ソフトウェア
1	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1
2	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	php 8.2.1

No9. ソフトウェア

CVE-2024-40898 - http_serverにおけるntlmハッシュの流出に関する脆弱性の検出

CVE-2024-40898 - A vulnerability related to ntlm hash leakage in http_server is Detected

高

1件

説明

Windows 上の Apache HTTP サーバにおいて、サーバ/vhost コンテキストで mod_rewrite を使用した SSRF を使用すると、 SSRF や悪意のあるリクエストを経由して NTML ハッシュを悪意のあるサーバに漏洩させる可能性があります。 この問題を修正したバージョン 2.4.62 へのアップグレードを推奨します。

解決方法

インストールされているソフトウェアパッケージをアップグレードしてください。

攻撃例

・CWE-918: Server-Side Request Forgery (SSRF)

脆弱なバージョン

2.4.0

参考資料

・http://www.openwall.com/lists/oss-security/2024/07/17/7
・https://security.netapp.com/advisory/ntap-20240808-0006/
・https://httpd.apache.org/security/vulnerabilities_24.html

対象のIT資産

No	アセット名	ドメイン名	使用ソフトウェア
1	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	http_server 2.4.58

No76. ソフトウェア

CVE-2011-0759 - wordpressにおけるCSRF攻撃に関する脆弱性の検出

CVE-2011-0759 - A vulnerability related to csrf attack in wordpress is Detected

中
1件

説明

Recaptcha (別名 WP-reCAPTCHA) プラグイン 2.9.8 の設定ページに複数のクロスサイトリクエストフォージェリ (CSRF) 脆弱性が存在します。2 for WordPress の設定ページにある複数のクロスサイトリクエストフォージェリ (CSRF) の脆弱性により、リモートの攻撃者は (1) recaptcha_opt_pubkey、(2) recaptcha_opt_privkey、(3) re_tabindex、(4) error_blank、(5) error_incorrect、(6) mailhide_pub、(7) mailhide_priv、(8) mh_replace_link、(9) mh_replace_title パラメータを経由して、管理者の認証を乗っ取ったり、クロスサイトスクリプティング (XSS) シーケンスを挿入したりします。

解決方法

インストールされているソフトウェアパッケージをアップグレードしてください。

攻撃例

・CWE-352: Cross-Site Request Forgery (CSRF)

参考資料

・http://secunia.com/advisories/43771
・https://exchange.xforce.ibmcloud.com/vulnerabilities/66169
・https://exchange.xforce.ibmcloud.com/vulnerabilities/66167
・http://www.securityfocus.com/bid/46909
・http://archives.neohapsis.com/archives/fulldisclosure/2011-03/0206.html

対象のIT資産

No	アセット名	ドメイン名	使用ソフトウェア
1	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	wordpress 6.4.2

No105. ソフトウェア

CVE-2020-1968 - openssIにおける盗聴に関する脆弱性の検出

CVE-2020-1968 - A vulnerability related to eavesdropping in openssl is Detected

低

2件

説明

ラクーン攻撃は、TLS仕様の欠陥を悪用したもので、ディフィー・ヘルマン（DH）ベースの暗号スイートが使用されている接続において、攻撃者がプレマスターの秘密を計算できてしまう可能性がある。このような場合、攻撃者はそのTLS接続で送信されるすべての暗号化通信を盗聴できることになる。この攻撃を悪用できるのは、実装が複数のTLS接続でDHシークレットを再利用する場合のみである。この問題はDH暗号スイートのみに影響し、ECDH暗号スイートには影響しないことに注意してください。この問題はOpenSSL 1.0.2に影響し、OpenSSL 1.0.2はサポートが終了し、パブリック・アップデートを受け取らなくなりました。OpenSSL 1.1.1にはこの問題に対する脆弱性はありません。OpenSSL 1.0.2w で修正されました (影響を受けるのは 1.0.2-1.0.2v)。

解決方法

インストールされているソフトウェアパッケージをアップグレードしてください。

攻撃例

・CWE-203: Observable Discrepancy

脆弱なバージョン

Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v)

参考資料

・https://usn.ubuntu.com/4504-1/
・https://www.oracle.com/security-alerts/cpuApr2021.html
・https://www.oracle.com/security-alerts/cpuapr2022.html
・https://security.netapp.com/advisory/ntap-20200911-0004/
・https://www.openssl.org/news/secadv/20200909.txt

対象のIT資産

No	アセット名	ドメイン名	使用ソフトウェア
1	54.199.229.228	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k
2	57.180.175.6	・www.vuln-ruhuna.net ・blog.vuln-ruhuna.net	openssl 1.0.2k

No110. ネットワーク

WAFの検出

WAF Detection is Detected

情報

1件

説明

ウェブアプリケーションファイアウォールが検出されました。

参考資料

・https://github.com/Ekultek/WhatWaf

対象のIT資産

No	アセット名
1	www.vuln-ruhuna.net

検出内容

内容 1.1	
検出名	apachegeneric
レスポンス	HTTP/1.1 200 OK Connection: close Content-Length: 165 Accept-Ranges: bytes Content-Type: text/html; charset=UTF-8 Date: Wed, 22 Jan 2025 00:31:02 GMT Etag: "a5-61df5abff215c" Last-Modified: Wed, 24 Jul 2024 03:14:10 GMT Server: Apache/2.4.58 () OpenSSL/1.0.2k-fips <html> <head> <meta charset="UTF-8"> <title>Test Page</title> <link rel="icon" href="favicon.html"> </head> <body> This is TEST </body> </html>