

# Raport z audytu bezpieczeństwa IT Global Manufacturer Inc.

---

Grandmetric Advanced Services

Wersja 1.0



## Kontrola wersji

Wersja	Data	Komentarze/Zmiany
1.0	13.09.2021	Wersja początkowa, Klasyfikacja: Confidential
1.0	24.09.2021	Finalna wersja dokumentu
1.0	27.06.2021	Podsumowanie dla kadry zarządzającej
1.0	28.06.2021	Podsumowanie znalezionych podatności
1.0	29.06.2021	Aktualizacja rekomendacji
1.0	29.06.2021	Klasyfikacja

## Spis treści

<b>1. PODSUMOWANIE DLA KADRY KIEROWNICZEJ.....</b>	<b>7</b>
<b>2. GŁÓWNE KONKLUZJE .....</b>	<b>8</b>
<b>3. GŁÓWNE REKOMENDACJE .....</b>	<b>9</b>
<b>4. PRZEDMIOT TESTÓW .....</b>	<b>10</b>
<b>5. RAMY CZASOWE TESTOWANIA .....</b>	<b>10</b>
<b>6. RISK RATING .....</b>	<b>11</b>
<b>7. METODOLOGIA I KRYTERIA TESTOWANIA .....</b>	<b>11</b>
<b>8. ZESTAW NARZĘDZI I METODY .....</b>	<b>11</b>
<b>9. PODSUMOWANIE ZNALEZIONYCH PODATNOŚCI.....</b>	<b>12</b>
<b>10. PODATNOŚCI W RAMACH GLOBAL MANUFACTURER.PL.....</b>	<b>16</b>
ZDOBYCIE CUDZEGO ADRESU POPRZEZ EDYCJĘ (C) .....	16
ENUMERACJA ADRESÓW UŻYTKOWNIKÓW (C).....	18
USUNIĘCIE CUDZEGO ADRESU (H) .....	21
STORED XSS W NAZWIE ADRESU (H) .....	24
STORED XSS W NAZWIE ZAMÓWIENIA (H).....	28
REFLECTED CROSS SITE SCRIPTING (H).....	30
BRAK NAGŁÓWKA HTTP 'STRICT-TRANSPORT-SECURITY' (M).....	33
NIEZABEZPIECZONE CIASTKA SESYJNE (M).....	35
CLICKJACKING (L) .....	37
ENUMERACJE UŻYTKOWNIKÓW (L).....	39
BŁĘDY MYSQL (L).....	44
OBSŁUGA NIEBEZPIECZNYCH WERSJI PROTOKOŁU TLS (L).....	47
NIEAKTUALNA WERSJA BIBLIOTEKI BOOTSTRAP (L) .....	47
NIEAKTUALNA WERSJA BIBLIOTEKI JQUERY (L) .....	50
NIEAKTUALNA WERSJA PHP (L).....	54
NIEAKTUALNA WERSJA BIBLIOTEKI VUE.JS (L) .....	56
BŁĘDY PHP (L) .....	58
RESET HASŁA W APLIKACJI (L).....	60
REJESTRACJA UŻYTKOWNIKA (L).....	63
BŁĘDY SOLR (L).....	65

REJESTRACJA NUMERÓW TELEFONÓW (L).....	68
CROSS SITE REQUEST FORGERY (L).....	69
<b>11. PODATNOŚCI I POTENCJALNE ZAGROŻENIA – APLIKACJE MOBILNE .....</b>	<b>74</b>
APK - ATAK PADDING ORACLE (L).....	74
PA - DOZWOLONY RUCH HTTP (L).....	75
BRAK OCHRONY PRZED ATAKAMI SŁOWNIKOWYMI (L).....	76
APLIKACJA POWINNA MONITOROWAĆ NIEAUTORYZOWANE PRÓBY DOSTĘPU ORAZ BLOKOWAĆ UŻYTKOWNIKA NA JAKIŚ CZAS PO PRZEKROCZENIU DANEJ LICZBY NIEUDANYCH PRÓB LOGOWANIA W KRÓTKIM CZASIE. ....	77
API - ENUMERACJA UŻYTKOWNIKÓW (L).....	77
REJESTRACJA UŻYTKOWNIKA (L).....	80
IPA - CERTIFICATE PINNING (L).....	82
NIEAUTORYZOWANY DOSTĘP DO KOMPONENTÓW APLIKACJI (L).....	82
<b>12. USŁUGI NA STYKU Z SIECIĄ INTERNET .....</b>	<b>84</b>
BŁĘDNA KONFIGURACJA CLOUDFLARE (H).....	84
WYSTAWIONE WRAŻLIWE USŁUGI (H).....	87
NIEBEZPIECZNA POLITYKA FLASH - CROSS DOMAIN POLICY (M).....	90
NIEZABEZPIECZONE COOKIES (M).....	91
BRAK NAGŁÓWKA HTTP 'STRICT TRANSPORT SECURITY' (M).....	93
NIEAKTUALNA WERSJA PROFTPD (M).....	94
NIEAKTUALNA WERSJA PHPMYADMIN (M).....	95
NIEAKTUALNA WERSJA SSH (M).....	97
AUTORYZACJA POP3 W SPOSÓB NIESZYFROWANY (M).....	98
BRAK OCHRONY PRZED ATAKAMI SŁOWNIKOWYMI (M).....	99
AUTORYZACJA SMTP W SPOSÓB NIESZYFROWANY (M).....	100
AUTORYZACJA POP3 W SPOSÓB NIESZYFROWANY (M).....	101
ENUMERACJA UŻYTKOWNIKÓW SSH (M).....	102
NIEAKTUALNA USŁUGA SSH (M).....	103
NIESZYFROWANA AUTORYZACJI HTTP BASIC AUTH (M).....	104
CLICKJACKING (L).....	105
DOSTĘPNY DEWELOPERSKI PANEL ADMINISTRATORA (L).....	107
DOSTĘPNY PANEL DIRECTADMIN (L).....	109
DOSTĘPNA STARA WERSJA WITRYNY (L).....	109
WYSTAWIONY STARY PANEL ADMINISTRATORA (L).....	111
NIEAKTUALNA WERSJA DIRECTADMIN (L).....	112
NIEAKTUALNA WERSJA BIBLIOTEKI JQUERY (L).....	113
NIEAKTUALNA WERSJA SERWERA NGINX (L).....	114

NIEAKTUALNA WERSJA ROUNDcube (L) .....	116
DOSTĘPNE PLIKI PHPINFO (L) .....	117
WYSTAWIONE OPROGRAMOWANIE PHPMyAdmin (L) .....	118
WYSTAWIONE OPROGRAMOWANIE RABBITMQ (L) .....	120
WYSTAWIONE OPROGRAMOWANIE ROUNDcube (L) .....	121
NIEBEZPIECZNA KONFIGURACJA USŁUGI SSH (L) .....	122
WŁĄCZONE ANONIMOWE SZYFROWANIE SSL (L) .....	123
WŁĄCZONA WERSJA TLS/1.0 (L) .....	124
<b>13. INFRASTRUKTURA SIECIOWA I DOSTĘP LAN, WAN, WI-FI .....</b>	<b>125</b>
NIEAUTORYZOWANY ODCZYT NFS (C) .....	125
WYKONANIE KODU PHP (C) .....	126
SERWER REDIS BEZ AUTORYZACJI (C) .....	129
NIEAUTORYZOWANY DOSTĘP DO KATALOGÓW SMB (C) .....	132
BRAK SEGMENTACJI SIECI LOKALNEJ (H) .....	142
STANDARDOWE UWIERZYTELNIENIE DRUKARKI (H) .....	146
NIEAUTORYZOWANA AKCJA Z WYKORZYSTANIEM SERWERA POCZTY SMTP (H) .....	148
BEZPIECZEŃSTWO I STABILNOŚĆ USŁUG SIECIOWYCH (H) .....	149
BRAK AUTORYZACJI DLA ISCSI (H) .....	152
NIEAKTUALNA WERSJA APACHE (H) .....	152
NIEAKTUALNE OPROGRAMOWANIE MIKROTIK (H) .....	154
BRAK AUTORYZACJI DO PANELU ZARZĄDZANIA DRUKARKĄ (H) .....	155
WYCIEK HASŁA DO SIECI WIFI (H) .....	159
DOSTĘP DO WRAŻLIWYCH USŁUG (H) .....	162
DOMYŚLNY 'COMMUNITY NAME' DLA SNMP (H) .....	163
NIEWSPIERANA WERSJA UNIX'A (H) .....	163
NIEWSPIERANA WERSJA MSSQL (H) .....	164
NIEWSPIERANA WERSJA PYTHON (H) .....	165
REKALKULACJA STP (M) .....	166
POŁĄCZENIE RDP BEZ NLA (M) .....	167
RDP MAN-IN-THE-MIDDLE (M) .....	168
SMB MAN-IN-THE-MIDDLE (M) .....	169
SNMP 'GETBULK' DDOS (M) .....	170
UŻYWANIE SZYFRÓW SSL O ŚREDNIEJ SIŁE (M) .....	171
DOSTĘPNE SSLV3 (M) .....	174
NIESZYFROWANY SERWER TELNET (M) .....	176
NIEAKTUALNA WERSJA JQUERY (L) .....	177
BRAK RESTRYKCJI LOGOWAŃ SSH (L) .....	178

DOSTĘPNE TLS/1.0 (L) .....	180
<b>14. REKOMENDACJE ARCHITEKTURY I FUNKCJI SIECIOWYCH.....</b>	<b>187</b>
BEZPIECZEŃSTWO .....	187
MECHANIZMY OCHRONY ANTI-SPOOFING .....	188
WEB APPLICATION FIREWALL.....	188
MONITORING LICZNIKÓW BROADCAST W SIECI I BUDOWANIE NORMY - KRZYWEJ .....	188
KONTROLA ZACHOWAŃ BROADCAST I BROADCAST STORM.....	188
CONTROL PLANE PROTECTION .....	189
MECHANIZM 802.1X DLA PORTÓW LAN .....	189
MECHANIZM 802.1X DLA SIECI WI-FI .....	189
MECHANIZM GUEST PORTAL REDIRECTION DLA PORTÓW LAN .....	189
AKTUALIZACJA OPROGRAMOWANIA I MODELI FIREWALL .....	190
WPROWADZENIE MECHANIZMÓW ANTI-MALWARE I IPS .....	190
MIKROSEGMENTACJA LUB / I SEGMENTACJA .....	190
BEZPIECZEŃSTWO IT .....	190
STABILNOŚĆ.....	191
VTP.....	191
VLAN1 / BRAK SEGMENTACJI .....	191
IMPLEMENTACJA ROUTINGU W SIECI WAN.....	191
IMPLEMENTACJA QoS .....	191
OPRACOWANIE STANDARYZACJI PORTÓW "UNIFIED" .....	192
AUTOMATYZACJA PROCESU ZARZĄDZANIA SIECIĄ.....	194
AUTOMATYZACJA KONFIGURACJI PORTÓW .....	194
AUTOMATYZACJA ZNAJDOWANIA DOSTĘPNYCH PORTÓW .....	194
WALIDACJA PROCESU PROVISIONING Z IPAM .....	195
CYKLICZNE ZBIERANIE DANYCH I BACKUP MANAGEMENT .....	195
MONITORING .....	195
LOGOWANIE .....	195
POWIADAMIANIE.....	196