Ogłoszenie nr 540085854-N-2020 z dnia 19-05-2020 r.

Warszawa:

OGŁOSZENIE O ZMIANIE OGŁOSZENIA

OGŁOSZENIE DOTYCZY:

Ogłoszenia o zamówieniu

INFORMACJE O ZMIENIANYM OGŁOSZENIU

Numer: 528946-N-2020

Data: 30/04/2020

SEKCJA I: ZAMAWIAJĄCY

Centralny Ośrodek Informatyki, Krajowy numer identyfikacyjny 10099948900000, ul. Aleje Jerozolimskie 132-136, 02-305 Warszawa, woj. mazowieckie, państwo Polska, tel. +48222502883, e-mail zamowienia.publiczne@coi.gov.pl, faks +48222502987.

Adres strony internetowej (url):

SEKCJA II: ZMIANY W OGŁOSZENIU

II.1) Tekst, który należy zmienić:

Miejsce, w którym znajduje się zmieniany tekst:

Numer sekcji: III.I.3

Punkt:

W ogłoszeniu jest: Określenie warunków: Wykonawca musi dysponować osobami, które zostaną skierowane przez Wykonawcę do realizacji Zamówienia, posiadającymi wskazane poniżej kwalifikacje zawodowe i doświadczenie:Część I: zespołem składającym się z 2 osób, z których każda posiada: I. doświadczenie w przeprowadzaniu analizy firmware'u urządzeń z wykorzystaniem technik inżynierii wstecznej, potwierdzone zgłoszeniem w okresie ostatniego roku co najmniej jednej podatności (CVE, PSV lub ICS-VU) dla rynkowych produktów. II. doświadczenie w wymiarze minimum 59 roboczodni (MD) w obszarze dotyczącym dekompozycji oprogramowania lub/i firmware'u urządzeń w okresie ostatnich dwóch lat do terminu składania ofert; Część II: zespołem składającym się z 6 osób, przy czym każda z nich musi posiadać: I. co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi

posiadać dwa różne certyfikaty spośród niżej wymienionych: 1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo ofensywne, 1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania, 1.3. Narzędzia bezpieczeństwa, 1.4. Techniki wykrywania błędów oprogramowania, 2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary: 2.1. Zbieranie informacji, 2.2. Inżynieria wsteczna dla aplikacji Android, 2.3. Wykorzystanie podatności w systemie Android, 2.4. Stosowanie zasad bezpieczeństwa, 2.5. Wady logiczne, 2.6. Szyfrowanie i kryptografia, 2.7. Identyfikacja podatnych implementacji, 3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary: 3.1. Procesy i metodologie testów penetracyjnych, 3.2. Analiza i inspekcja aplikacji WEB, 3.3. Gromadzenie informacji, 3.4. Zarządzanie podatnościami WEB aplikacji, 3.5. OWASP Testing Guide / OWASP Top 10, 3.6. Manualne potwierdzenie podatności XSS, SQLi itd., 3.7. Zaawansowane raportowanie i remediacja, 4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary: 4.1. Procesy i metodologie testów penetracyjnych, 4.2. Analiza i kontrola aplikacji WEB, 4.3. Zaawansowane umiejętności raportowania i działań naprawczych, 4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd., 4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych, 4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą, 5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary: 5.1. Ataki na aplikacje webowe (min. XSS/LFI), 5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE, 5.3. Omijanie systemów antywirusowych, 5.4. Omijanie mechanizmów zabezpieczenia pamięci, 5.5. Fuzzing, konstruowanie exploitów 0-day, 5.6. Obchodzenie zabezpieczeń, 5.7. Atakowanie infrastruktury sieciowej, 6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary: 6.1. Analiza oraz ocena ryzyka danych oraz systemów, 6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom, 6.3. Znajomość narzędzi, systemów, programów, 6.4. Znajomość procedur oraz metodologii, 6.5. Znajomość Regulacji i polityk. II. doświadczenie w wymiarze minimum 119 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa obszaru aplikacji w okresie ostatnich dwóch lat do terminu składania ofert; Część III: zespołem składającym się z 4 osób, przy czym każda z nich musi posiadać: I. co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi posiadać dwa różne certyfikaty spośród niżej wymienionych: 1. aktualny certyfikat Offensive Security Certified

Professional (OSCP) lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo ofensywne, 1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania, 1.3. Narzędzia bezpieczeństwa, 1.4. Techniki wykrywania błędów oprogramowania, 2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary: 2.1. Zbieranie informacji, 2.2. Inżynieria wsteczna dla aplikacji Android, 2.3. Wykorzystanie podatności w systemie Android, 2.4. Stosowanie zasad bezpieczeństwa, 2.5. Wady logiczne, 2.6. Szyfrowanie i kryptografia, 2.7. Identyfikacja podatnych implementacji, 3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary: 3.1. Procesy i metodologie testów penetracyjnych, 3.2. Analiza i inspekcja aplikacji WEB, 3.3. Gromadzenie informacji, 3.4. Zarządzanie podatnościami WEB aplikacji, 3.5. OWASP Testing Guide / OWASP Top 10, 3.6. Manualne potwierdzenie podatności XSS, SQLi itd., 3.7. Zaawansowane raportowanie i remediacja, 4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary: 4.1. Procesy i metodologie testów penetracyjnych, 4.2. Analiza i kontrola aplikacji WEB, 4.3. Zaawansowane umiejętności raportowania i działań naprawczych, 4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd., 4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych, 4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą, 5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary: 5.1. Ataki na aplikacje webowe (min. XSS/LFI), 5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE, 5.3. Omijanie systemów antywirusowych, 5.4. Omijanie mechanizmów zabezpieczenia pamięci, 5.5. Fuzzing, konstruowanie exploitów 0-day, 5.6. Obchodzenie zabezpieczeń, 5.7. Atakowanie infrastruktury sieciowej, 6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary: 6.1. Analiza oraz ocena ryzyka danych oraz systemów, 6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom, 6.3. Znajomość narzędzi, systemów, programów, 6.4. Znajomość procedur oraz metodologii, 6.5. Znajomość Regulacji i polityk. II. doświadczenie w wymiarze minimum 119 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa obszaru infrastruktury w okresie ostatnich dwóch lat do terminu składania ofert; Część IV: zespołem składającym się z 3 osób, w tym co najmniej 1 osoba posiadająca łącznie: I. poniższe kompetencje, certyfikaty: 1. Aktualny certyfikat Certified Information Security Professional (CISSP) wydany przez ISC2 lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo i zarządzanie ryzykiem, 1.2. Bezpieczeństwo telekomunikacji i sieci, 1.3.

Obsługa incydentów, 1.4. Testy bezpieczeństwa, 1.5. Bezpieczeństwo oprogramowania, 1.6. Zarządzanie tożsamością i dostępami, 2. Aktualny certyfikat CSSLP lub równoważny, który pokrywa obszary: 2.1. Wymagania bezpieczeństwa, 2.2. Projektowanie bezpiecznego oprogramowania, 2.3. Wytwarzanie bezpiecznego kodu źródłowego, 2.4. Testowanie bezpieczeństwa oprogramowania, 2.5. Wdrażanie i utrzymanie bezpiecznego oprogramowania. II. doświadczenie w wymiarze minimum 59 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa kodu źródłowego w okresie ostatnich dwóch lat do terminu składania ofert; **W ogłoszeniu powinno być:** Określenie warunków: Wykonawca musi dysponować osobami, które zostaną skierowane przez Wykonawcę do realizacji Zamówienia, posiadającymi wskazane poniżej kwalifikacje zawodowe i doświadczenie:Część I: zespołem składającym się z 2 osób, z których każda posiada: I. doświadczenie w przeprowadzaniu analizy firmware'u urządzeń z wykorzystaniem technik inżynierii wstecznej, potwierdzone zgłoszeniem w okresie ostatnich trzech lat co najmniej jednej podatności (CVE, PSV lub ICS-VU) dla rynkowych produktów. II. doświadczenie w wymiarze minimum 59 roboczodni (MD) w obszarze dotyczącym dekompozycji oprogramowania lub/i firmware'u urządzeń w okresie ostatnich dwóch lat do terminu składania ofert; Część II: zespołem składającym się z 6 osób, przy czym każda z nich musi posiadać: I. co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi posiadać dwa różne certyfikaty spośród niżej wymienionych: 1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo ofensywne, 1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania, 1.3. Narzędzia bezpieczeństwa, 1.4. Techniki wykrywania błędów oprogramowania, 2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary: 2.1. Zbieranie informacji, 2.2. Inżynieria wsteczna dla aplikacji Android, 2.3. Wykorzystanie podatności w systemie Android, 2.4. Stosowanie zasad bezpieczeństwa, 2.5. Wady logiczne, 2.6. Szyfrowanie i kryptografia, 2.7. Identyfikacja podatnych implementacji, 3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary: 3.1. Procesy i metodologie testów penetracyjnych, 3.2. Analiza i inspekcja aplikacji WEB, 3.3. Gromadzenie informacji, 3.4. Zarządzanie podatnościami WEB aplikacji, 3.5. OWASP Testing Guide / OWASP Top 10, 3.6. Manualne potwierdzenie podatności XSS, SQLi itd., 3.7. Zaawansowane raportowanie i remediacja, 4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary: 4.1. Procesy i metodologie testów penetracyjnych, 4.2. Analiza i kontrola aplikacji WEB, 4.3. Zaawansowane umiejętności

raportowania i działań naprawczych, 4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd., 4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych, 4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą, 5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary: 5.1. Ataki na aplikacje webowe (min. XSS/LFI), 5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE, 5.3. Omijanie systemów antywirusowych, 5.4. Omijanie mechanizmów zabezpieczenia pamięci, 5.5. Fuzzing, konstruowanie exploitów 0-day, 5.6. Obchodzenie zabezpieczeń, 5.7. Atakowanie infrastruktury sieciowej, 6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary: 6.1. Analiza oraz ocena ryzyka danych oraz systemów, 6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom, 6.3. Znajomość narzędzi, systemów, programów, 6.4. Znajomość procedur oraz metodologii, 6.5. Znajomość Regulacji i polityk. II. doświadczenie w wymiarze minimum 119 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa obszaru aplikacji w okresie ostatnich dwóch lat do terminu składania ofert; Część III: zespołem składającym się z 4 osób, przy czym każda z nich musi posiadać: I. co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół musi posiadać dwa różne certyfikaty spośród niżej wymienionych: 1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo ofensywne, 1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania, 1.3. Narzędzia bezpieczeństwa, 1.4. Techniki wykrywania błędów oprogramowania, 2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary: 2.1. Zbieranie informacji, 2.2. Inżynieria wsteczna dla aplikacji Android, 2.3. Wykorzystanie podatności w systemie Android, 2.4. Stosowanie zasad bezpieczeństwa, 2.5. Wady logiczne, 2.6. Szyfrowanie i kryptografia, 2.7. Identyfikacja podatnych implementacji, 3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary: 3.1. Procesy i metodologie testów penetracyjnych, 3.2. Analiza i inspekcja aplikacji WEB, 3.3. Gromadzenie informacji, 3.4. Zarządzanie podatnościami WEB aplikacji, 3.5. OWASP Testing Guide / OWASP Top 10, 3.6. Manualne potwierdzenie podatności XSS, SQLi itd., 3.7. Zaawansowane raportowanie i remediacja, 4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary: 4.1. Procesy i metodologie testów penetracyjnych, 4.2. Analiza i kontrola aplikacji WEB, 4.3. Zaawansowane umiejętności raportowania i działań naprawczych, 4.4. Zaawansowana wiedza i umiejętności omijania

podstawowych oraz zaawansowanych filtrów XSS, SQLi itd., 4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych, 4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą, 5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary: 5.1. Ataki na aplikacje webowe (min. XSS/LFI), 5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE, 5.3. Omijanie systemów antywirusowych, 5.4. Omijanie mechanizmów zabezpieczenia pamięci, 5.5. Fuzzing, konstruowanie exploitów 0-day, 5.6. Obchodzenie zabezpieczeń, 5.7. Atakowanie infrastruktury sieciowej, 6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary: 6.1. Analiza oraz ocena ryzyka danych oraz systemów, 6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom, 6.3. Znajomość narzędzi, systemów, programów, 6.4. Znajomość procedur oraz metodologii, 6.5. Znajomość Regulacji i polityk. II. doświadczenie w wymiarze minimum 119 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa obszaru infrastruktury w okresie ostatnich dwóch lat do terminu składania ofert; Część IV: zespołem składającym się z 3 osób, w tym co najmniej 1 osoba posiadająca łącznie: I. poniższe kompetencje, certyfikaty: 1. Aktualny certyfikat Certified Information Security Professional (CISSP) wydany przez ISC2 lub równoważny, który pokrywa obszary: 1.1. Bezpieczeństwo i zarządzanie ryzykiem, 1.2. Bezpieczeństwo telekomunikacji i sieci, 1.3. Obsługa incydentów, 1.4. Testy bezpieczeństwa, 1.5. Bezpieczeństwo oprogramowania, 1.6. Zarządzanie tożsamością i dostępami, 2. Aktualny certyfikat CSSLP lub równoważny, który pokrywa obszary: 2.1. Wymagania bezpieczeństwa, 2.2. Projektowanie bezpiecznego oprogramowania, 2.3. Wytwarzanie bezpiecznego kodu źródłowego, 2.4. Testowanie bezpieczeństwa oprogramowania, 2.5. Wdrażanie i utrzymanie bezpiecznego oprogramowania. II. doświadczenie w wymiarze minimum 59 roboczodni (MD) w obszarze dotyczącym testów bezpieczeństwa kodu źródłowego w okresie ostatnich dwóch lat do terminu składania ofert;

Miejsce, w którym znajduje się zmieniany tekst:

Numer sekcji: IV.6.2.

Punkt:

W ogłoszeniu jest: Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu: Data: 2020-05-20, godzina: 11:00

W ogłoszeniu powinno być: Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu: Data: 2020-05-27, godzina: 11:00