Bitdefender

Wymeldowanie za dodatkową opłatą – wyjaśniono luki w silniku rezerwacji hoteli

13.09.2023

Silniki rezerwacyjne – dzięki nim świat podróży i hotelarstwa bardzo szybko się rozwija. Silniki rezerwacji hoteli stanowią kluczową, prawie niewidoczną część branży hotelarsko-gastronomicznej, a ich bezpieczeństwo jest niezbędne, aby chronić dane osobowe i finansowe gości. Czasami technologia rezerwacji pada ofiarą zmotywowanych cyberprzestępców, którzy wykorzystują luki w kodzie, aby uzyskać dostęp do poufnych informacji o kliencie, takich jak imię i nazwisko, adres, adres e-mail, numer telefonu, numer karty kredytowej lub debetowej, data ważności oraz kod zabezpieczający lub kod weryfikacyjny karty. Firma Bitdefender jakiś czas temu ujawniła lukę w silniku rezerwacyjnym i przekazała tę informację do producenta oprogramowania. Komunikat pozostał bez odpowiedzi, dlatego producent oprogramowania postanowił zastosować otwarty apel do użytkowników IRM Next Generation o szczególną ostrożność.

Niebezpieczne luki w silniku rezerwacji hoteli

W 2021 roku został wykryty cyberatak na silnik rezerwacji online IRM Next Generation zbudowany przez Resort Data Processing, Inc. („RDP"). Atak ten prawdopodobnie nie jest odosobniony wśród szerokiej gamy silników rezerwacji online zbudowanych przez różnych innych producentów oprogramowania. Jednakże jest to ściśle powiązane ze śledztwem, w którym wezwano Bitdefender o pomoc. Nawiasem mówiąc, wyniki dochodzenia pomogły zespołowi do spraw cyberbezpieczeństwa rumuńskiej firmy zrozumieć, w jaki sposób miał miejsce cyberatak na IRMNg w 2021 r. Zespół Bitdefender postanowił podzielić się wynikami uzyskanymi podczas badania tego cyberataku, aby pomóc innym podmiotom gospodarczym zachować ochronę.

Atak na pierwszy rzut oka

Badając anomalną aktywność, badacze Bitdefender znaleźli złośliwe pliki na serwerach, na których działa silnik rezerwacji online IRM Next Generation zbudowany przez Resort Data Processing, Inc.

Dochodzenie Bitdefender ujawnia zakres ataku i zarysowuje kilka luk w zabezpieczeniach mechanizmu rezerwacji online IRM Next Generation, które zostały zidentyfikowane, skatalogowane oraz zgłoszone podatnemu dostawcy zgodnie z harmonogramem poniżej.

Zidentyfikowane podatności

CVE-2023-39420 — Użycie zakodowanych na stałe poświadczeń w pliku RDPCore.dll (CWE-798)

CVE-2023-39421 — Użycie zakodowanych na stałe poświadczeń w pliku RDPWin.dll CWE-798)

CVE-2023-39422 — Użycie zakodowanych na stałe poświadczeń w punktach końcowych /irmdata/api/ (CWE-798)

CVE-2023-39423 — Niewłaściwa neutralizacja elementów specjalnych używanych w poleceniu SQL w pliku RDPData.dll (CWE-89)

CVE-2023-39424 — Niewłaściwa neutralizacja specjalnych elementów na wyjściu używanych przez dalszy komponent („wstrzykiwanie”) w pliku RDPngFileUpload.dll (CWE-74)

Harmonogram ujawnień

Kwiecień-maj 2023 – Bitdefender identyfikuje problemy w wielu komponentach aplikacji IRMNg podczas badania infekcji złośliwym oprogramowaniem.

23 maja 2023 r. – Bitdefender podejmuje pierwszą próbę kontaktu z podatnym dostawcą za pośrednictwem poczty elektronicznej.

30 maja 2023 r. – Biorąc pod uwagę, że poprzednia próba nie przyniosła żadnego rezultatu, Bitdefender podejmuje drugą próbę za pośrednictwem poczty elektronicznej.

02 sierpnia 2023 – Bitdefender przydziela numery CVE zidentyfikowanym podatnościom.

16 sierpnia 2023 r. – Bitdefender w dalszym ciągu kontaktuje się z podatnym dostawcą za pośrednictwem Twittera i Facebooka.

7 września 2023 r. – Niniejszy raport zostaje upubliczniony w ramach programu odpowiedzialnego ujawniania informacji.

Odpowiedzialne ujawnianie

„Wzywamy wszystkie firmy korzystające z podatnych na ataki wersji silnika IRMNG, aby oceniły wpływ tych luk i podjęły odpowiednie działania (szczegółowe informacje na temat ataku można również znaleźć na naszym blogu Business Insights)" – brzmi komunikat firmy Bitdefender.

„Raport i otwarty apel firmy Bitdefender do użytkowników IRM Next Generation to dowód pokazujący, że wiele firm nadal nie podchodzi odpowiedzialnie do kwestii cyberbezpieczeństwa swoich produktów. Dlatego powinniśmy zawsze korzystać tylko z urządzeń, które zostały zabezpieczone skutecznym systemem antywirusowym" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/wymeldowanie-za-dodatkowa-oplata-

wyjasniono-luki-w-silniku-rezerwacji-hoteli/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.09.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.