Windows 10 में DPAPI सुरक्षा दोष

पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

1 Windows 10 में DPAPI सुरक्षा दोष

1.1 संक्षिप्त विवरण

हमारे विशेषज्ञों ने DPAPI सुरक्षा में एक नया गंभीर दोष पाया है, जो किसी को भी Windows 10 में अंतिम एक्टिव यूजर्स के (DPAPI द्वारा संरक्षित) व्यक्तिगत डेटा को डिक्रिप्ट करने की अनुमति देता है।

1.2 कौन से OS प्रभावित होते हैं?

यह खामी Windows 10 को प्रभावित करती है, जिसकी शुरुआत 1709फॉल क्रिएटर्स अपडेट से होती है, साथ ही Windows 10 के पिछले वर्जन में माइक्रोसॉफ्ट अकाउन्ट्स में अब तक सिस्टम वॉल्यूम एन्क्रिप्शन सक्रिय है।

1.3 DPAPI क्या है?

डेटा प्रोटेक्शन एप्लिकेशन प्रोग्रामिंग इंटरफेस (DPAPI) का उद्देश्य उपयोगकर्ता के व्यक्तिगत डेटा, एन्क्रिप्शन की, सिस्टम के महत्वपूर्ण डेटा, साथ ही अन्य संवेदनशील जानकारी का सुरक्षित एन्क्रिप्शन करना है। यह Windows 2000 के बाद से सभी विंडोज ऑपरेटिंग सिस्टम में एक प्राथमिक सुरक्षा सबसिस्टम है। DPAPI मुख्य रूप से लोकप्रिय हो गया है क्योंकि इसका उपयोग करना आसान है, क्योंकि इसमें संवेदनशील डेटा को एन्क्रिप्ट या डिक्रिप्ट करने के लिए केवल दो कार्य होते हैं: CryptProtectData और CryptUnprotectData। यह सरल लग सकता है लेकिन CryptProtectData/CryptUnprotectData का आंतरिक तर्क काफी जटिल है। आपइस लेख में DPAPI के काम करने के तरीके के बारे में अधिक पढ़ सकते हैं।

1.4 पिछली DPAPI कमजोरियां

DPAPI को सुरक्षा के कई पहलुओं को ध्यान में रखते हुए बनाया गया था और निश्चित रूप से इसे सर्वश्रेष्ठ डेटा सुरक्षा प्रणालियों में से एक माना जा सकता है, जो इस बात का अच्छा उदाहरण है कि एक अच्छी तरह से डिज़ाइन किया गया उत्पाद कई वर्षों तक कैसे काम कर सकता है। हालांकि, पहले वर्जन में गंभीर समस्याएं थीं। समस्या इस तथ्य के कारण थी कि DPAPI v1 में प्राथमिक एन्क्रिप्शन की यूजर्स के पासवर्ड के NTLM हैश पर आधारित थी। इसका मतलब यह था कि NTLM हैश (जो SAM रजिस्ट्री में संग्रहीत था) तक प्रवेश प्राप्त करने के लिए पर्याप्त था ताकि DPAPI द्वारा संरक्षित सभी पासवर्ड और डेटा को डिक्रिप्ट किया जा सके। सौभाग्य से, माइक्रोसॉफ्ट ने तुरंत तर्क में दोष पाया और दूसरा DPAPI संशोधन जल्दी से शुरू किया, जो अब तक सही ढंग से चल रहा है।

नई कमजोरियां निम्नलिखित चीजों को छोड़कर पहली समस्या के समान है:

- नई DPAPI समस्या केवल सिस्टम के अंतिम सक्रिय यूजर को प्रभावित करती है
- यह डोमेन अकाउन्ट्स पर लागू नहीं होता
- पहले वर्जन के विपरीत, नई कमजोरी कोई डेवलपर की गलती नहीं है, बल्कि सुरक्षा और उपयोगिता पर एक मजबूर समझौता है, इसलिए बोलने के लिए।

1.5 ऑटोमेटिक रिस्टार्ट साइन-ऑन (ARSO) क्या है?

Windows 8 से शुरू होकर, अबलॉक स्क्रीन एप्लिकेशनलॉन्च करना संभव है। यही है, ऐसे एप्लिकेशन जो यूजर्स के सत्र के लॉक होने पर सूचनाएं शुरू करते हैं, काम करते हैं और प्रदर्शित करते हैं। उदाहरण के लिए, कैलेंडर अपॉइंटमेंट, सूचनाएं, ईमेल, संदेश आदि। हालांकि, अपग्रेड के बाद ऑटोमेटिक रीबूट के दौरान, ये एप्लिकेशन काम करना बंद कर देंगे क्योंकि उन्हें एक सक्रिय यूजर सत्र की आवश्यकता होती है। एक स्पष्ट सुरक्षा संघर्ष है जिसे माइक्रोसोफ्ट द्वारा मूल तरीके से हल किया गया है।

सिस्टम द्वारा ओटोमेटिक रीबूट शुरू करने से ठीक पहले, वर्तमान यूजर क्रेडेंशियल एक विशेष LSA रहस्य में संग्रहीत किए जाते हैं। रिबूट करने के बाद, इन क्रेडेंशियल्स का उपयोग उपयोगकर्ता को स्वचालित रूप से लॉग इन करने और एक सक्रिय सत्र बनाने के लिए किया जाता है, लेकिन जब तक वह पासवर्ड, पिन आदि दर्ज नहीं करता है, तब तक यूजर के लिए इंटरैक्टिव भाग उपलब्ध नहीं होगा। इस प्रकार, यूजर का अंतिम सत्र ऑटोमेटिक रूप से पुनर्स्थापित होगा और लॉक स्क्रीन एप्लिकेशन काम करेंगे। इस प्रकार ऑटोमेटिक रिस्टार्ट साइन-ऑन सिस्टम संक्षेप में काम करता है।

1.6 ट्रस्टेड बूट ऑटो-लॉगऑन (TBAL) क्या है

Windows 10 में, ARSO ट्रस्टेड बूट ऑटो-लॉगऑन (TBAL) तंत्र का उपयोग करता हैऑटो-लॉगऑनएक विंडोज बिल्ट-इन फीचर है जो उपयोगकर्ताओं को उनके नाम और पासवर्ड दर्ज करने की प्रतीक्षा करने के बजाय स्वचालित रूप से लॉग ऑन करने की अनुमति देता है। ऑटोलॉगन रजिस्ट्री के माध्यम से सक्रिय होता है जहां आपको उपयोगकर्ता का क्लियरटेक्स्ट पासवर्ड डालना होगा। स्टार्टअप के दौरान, सिस्टम विकल्प की जांच करता है और यदि यह सेट है, तो प्लेनटेक्स्ट पासवर्ड पढ़ता है और लॉगऑन करने के लिए इसका उपयोग करता है।

Windows 10 में ऑटोलॉगन को TBAL मिकेनिजम के साथ बढ़ाया गया था। TBAL एक सामान्य ऑटोलॉगन और ARSO सुविधाओं का एक प्रकार का सहजीवन है। हालांकि: लेकिन इसमें कई अंतर हैं|

- TBAL रेग्युलर और माइक्रोसॉफ्ट दोनों अकाउन्ट्स को सपोर्ट करता है
- TBAL द्वारा कोई सरल शब्दों में पासवर्ड संग्रहीत नहीं किया जाता है
- ऐसा लगता है कि TBAL अनुरोध पर ही नहीं, बल्कि हमेशा चालू रहता है। हालांकि Windows 10 के पहले वर्जनो में, सिस्टम ने पूर्ण डिस्क एन्क्रिप्शन सक्षम होने के बाद ही TBAL को सक्रिय किया।

तो TBAL कैसे काम करता है?

1.7 TBAL कैसे काम करता है?

शट डाउन करने से पहले, LSA प्रक्रिया LSA secret DefaulPassword में एक विशेष टेक्स्ट वेल्यु _TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9} सेव करती है, यह एक संकेत है कि यह एक सामान्य ऑटोलॉगन पासवर्ड नहीं है बल्कि इसके बजाय एक TBAL टोकन है। फिर, सक्रिय यूजर अकाउन्ट के प्रकार के आधार पर, एक और LSA रहस्य बनाया जाता है। यदि यह एक ऑफ़लाइन अकाउन्ट है, तो सिस्टम यूजर नाम, NTLM, SHA1 पासवर्ड हैश के साथ कुछ अन्य निजी जानकारी को M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA नाम के LSA सीक्रेट में संग्रहीत करता है। अगर यह एक माइक्रोसोफ्ट अकाउन्ट है, तो या तो M$_CLOUDAP_TBAL_{8283D8D4-55B6-466F-B7D7-17A1352D9CAB}_<UID> (Windows 1607 और पुराने) या M$_CLOUDAP_TBAL_{4416F0BD-3A59-4590-9579-DA6E08AF19B3} UID> (Windows 1703 और बाद में) सीक्रेट बनाया जाता है, जहां <UID> यूनिक यूजर आईडी का SHA256 हैश है। ऑफ़लाइन

अकाउन्ट के रहस्य के विपरीत, इसमें केवल 96-बाइट एन्क्रिप्शन की होती है जो DPAPI प्राथमिक की प्राप्त करने के लिए आवश्यक होती है।

PC रीबूट होने के बाद, सिस्टम TBAL टोकन की पहचान करता है और उपयोगकर्ता के SHA1 हैश (ऑफ़लाइन अकाउन्ट के लिए) या 96-बाइट की का उपयोग करके DPAPI प्रायमरी की को डिक्रिप्ट करता है यदि यह एक माइक्रोसॉफ्ट अकाउन्ट है। फिर LSA टोकन और LSA की रहस्य दोनों हटा दिए जाते हैं।

यदि सिस्टम हाइबरनेट कर रहा है या यूजर को साइन आउट कर रहा है, तो TBAL टोकन नहीं लिखा जाता है, बल्कि केवल रिबूट या शटडाउन पर लिखा जाता है।

1.8 समस्या का कारण क्या है?

यूजर के लिए समस्या यह है कि सिस्टम बंद होने के बाद, कोई भी व्यक्ति जिसके पास PC तक भौतिक पहुंच है, वह DPAPI प्रायमरी की को डिक्रिप्ट करने के लिए संग्रहीत TBAL रहस्य का उपयोग कर सकता है और इसके परिणामस्वरूप, उपयोगकर्ता के सभी डेटा जो DPAPI का उपयोग करके एन्क्रिप्ट किया गया है। यह स्पष्ट है कि कमजोरी का कारण गलत तर्क नहीं है, बल्कि विंडोज सुरक्षा के लिए माइक्रोसॉफ्ट का वैचारिक दृष्टिकोण है, जो पहले DPAPI कार्यान्वयन में पाया गया था पासवर्ड-मुक्त लॉगिन कार्यान्वयन में पिछली त्रुटियों के विपरीत था। हालाँकि, यह हाल के वर्षों की एक वैश्विक प्रवृत्ति प्रतीत होती है।

1.9 कौन सा डेटा जोखिम में है?

- लोकप्रिय इंटरनेट ब्राउज़र द्वारा सेव किये गए नेटवर्क पासवर्ड: Google Chrome, Internet Explorer, Microsoft Edge, Opera, आदि।
- ईमेल क्लाइंट के पासवर्ड: Microsoft Office Outlook, Windows Mail
- साझा किए गए फ़ोल्डरों और संसाधनों के पासवर्ड
- विंडोज वॉल्ट में संग्रहीत पासवर्ड, कीज और अन्य निजी डेटा
- रिमोट डेस्कटॉप पासवर्ड
- EFS प्राइवेट कीज और इस प्रकार EFS एन्क्रिप्टेड फाइलों तक पहुंच
- S-MIME मेल में एन्क्रिप्शन कीज
- यूजर्स के प्रमाणपत्र
- क्रेडेंशियल मैनेजर में संगृहीत नेटवर्क पासवर्ड
- किसी भी एप्लिकेशन, जैसे Skype, Windows Rights Management Services, Windows Media, MSN messenger, Google Talk, आदि में CryptProtectData API का उपयोग करके सुरक्षित कोई भी व्यक्तिगत डेटा।

1.10 PoC

यह वीडियो दर्शाता है कि Windows 10 में अपने लॉगिन पासवर्ड को जाने बिना अंतिम सक्रिय यूजर के व्यक्तिगत डेटा तक पहुंचना कितना आसान है। हालांकि यह माना जाता है कि कोई भी मालिक के लॉगऑन पासवर्ड को जाने बिना ऐसा नहीं कर सकता

है,Windows Vault में संग्रहीत और DPAPI द्वारा संरक्षित Facebook क्रेडेंशियल्स को डिक्रिप्ट करने के लिए प्रोग्राम गुप्त TBAL सीक्रेट्स का उपयोग करता है।

1.11 निष्कर्ष

जैसा कि हमनेअपने पिछले लेख में चेतावनी दी थीविंडोज के अगले वर्जन में अंतिम-यूज़र के लिए सुरक्षा सुनिश्चित करने पर कम से कम केंद्रित होंगे। वे उपयोगकर्ता जिनके लिए अधिकतम स्तर की सुरक्षा प्रदान करना महत्वपूर्ण है, उन्हें SYSKEY स्टार्टअप पासवर्ड या पूर्ण डिस्क एन्क्रिप्शन सेट के साथ 1709वर्जन तक Windows 10 के साथ एक ऑफ़लाइन अकाउन्ट स्थापित करने की अनुशंसा की जाती है।