K jakým údajům byl přístup?

support.lastpass.com/help/what-data-was-accessed

Níže je podrobnější popis zákaznických dat LastPass ovlivněných dvěma bezpečnostními incidenty.

Poznámka: Chcete-li si přečíst úplnou aktualizaci bezpečnostního incidentu od našeho generálního ředitele Karima Toubby, navštivte blog LastPass .

I. Tajemství zákaznických účtů, klíče API a informace o integraci třetích stran

V závislosti na konkrétní konfiguraci a integracích účtu LastPass zákazníka mohou data uložená v zálohách, ke kterým přistupuje aktér hrozby, zahrnovat tajemství, klíče a integrační informace specifické pro LastPass a/nebo třetí strany. Mnoho z těchto položek platí pouze v případě, že zákazník LastPass využívá tyto specifické funkce, integrace nebo konfigurace účtu:

Typ dotčeného uživatele	Tajemství zákazníka	Popis
Spotřebitelé a firemní zákazníci (nefederovaný)	Semena multifaktorové autentizace (MFA).	Semena MFA přiřazená uživateli, když poprvé zaregistroval svůj vybraný vícefaktorový autentizátor pro ověření k trezoru LastPass.
Hashe dočasných (jednorázových) hesel (OTP) a jednorázových hesel pro obnovení účtu (rOTP)		Hash zákazníka generovaného OTP a/nebo účtu rOTP. Z velké opatrnosti LastPass tyto hashe proaktivně zrušil.
Firemní zákazníci (pouze federace)	Klíč rozdělené znalosti (“K2”).	Klíče K2 uložené v LastPass jsou kombinovány s klíči K1 uloženými u poskytovatele identity zákazníka (IdP) pro konfiguraci nasazení federovaného přihlášení. Tento model rozdělených znalostí byl zvolen k obraně proti této specifické situaci. Aktér ohrožení by potřeboval přístup ke komponentám K1 i K2, aby se pokusil dešifrovat offline trezor. Nastavení zabezpečení poskytovatele identity třetích stran přímo ovlivňuje dostupnost a zabezpečení komponent K1.
Firemní zákazníci (nefederovaný)	Tajemství integrace MFA API	Tajné informace používané k integraci dodavatelů MFA třetích stran (např. Duo Security, RSA SecurID, SecureAuth) s LastPass.
Firemní zákazníci (nefederovaný)	Časově založené jednorázové heslo (TOTP) semena	Semena používaná ke generování ověřovacích kódů TOTP pro Google Authenticator, Microsoft Authenticator, LastPass Authenticator a Grid.
Firemní zákazníci	Tajemství integrace Splunk Security Information & Event Management (SIEM).	Tajemství používaná k umožnění odesílání protokolů událostí LastPass do instance Splunk zákazníka, která poskytuje auditování/monitorování událostí LastPass.
Firemní zákazníci	„Push“ přihlašovací údaje webu	Přihlašovací údaje, které mohly být uživateli nebo skupině LastPass „předány“ obchodním administrátorem LastPass.
Firemní zákazníci	SCIM, Enterprise API a klíče SAML	Klíče API používané správci a uživateli LastPass Business k integraci s adresářovými službami třetích stran, správě a poskytování/de-provision uživatelům a využívání jednotného přihlášení (SSO). Uživatelé těchto klíčů byli již dříve kontaktováni společností LastPass v prosinci 2022 s konkrétními pokyny k nápravě, jak je resetovat.

Přístup k těmto tokenům, klíčům a semínkům API představuje různá rizika. Aktér hrozby by mohl potenciálně obejít určitou službu, přistupovat k určité aplikaci nebo manipulovat s daty. Kde to bylo možné, LastPass podnikl kroky k nápravě těchto rizik zrušením platnosti určitých klíčů a rozhraní API. Bulletiny zabezpečení poskytované v souvislosti s touto aktualizací blogu popisují akce, které již LastPass podnikl, a také akce, které mohou zákazníci potřebovat k další nápravě rizik ve svém vlastním prostředí.

II. Databáze zákazníků LastPass

Aktér hrozby dokázal zkopírovat zálohu naší zákaznické databáze ze dne 14. srpna 2022. Žádné účty vytvořené po tomto datu nejsou ovlivněny. Databáze zákazníků obsahovala nešifrované základní informace o zákaznických účtech a související metadata včetně:

Typ uživatele LastPass	Datové pole	Popis
Uživatelé Business & Teams	fakturační adresa	Obchodní fakturační adresa
Jméno společnosti	Název firmy	
A/Tax ID	EIN/daňové ID společnosti nebo firmy	
Emailová adresa	Firemní e-mailová adresa uživatele (např. jméno@lastpass.com)	
Jméno koncového uživatele	Jméno koncového uživatele (pokud je uvedeno)	
IP adresa	IP adresy důvěryhodných zařízení, ze kterých koncoví uživatelé přistupovali ke službě LastPass	
Telefonní číslo	Číslo mobilního telefonu používané pro obnovení SMS (pokud je povoleno)	
Jedinečný identifikátor mobilního zařízení	Jedinečný identifikátor jakéhokoli mobilního zařízení používaného pro přístup ke službě LastPass	
Iterace PBKDF2 SHA256	Počet iterací PBKDF2, pro které byl zákazník nakonfigurován	
Bezplatní, prémioví a rodinní uživatelé	fakturační adresa	Fakturační adresa (pokud je uvedena)
Emailová adresa	E-mailová adresa koncového uživatele	
Jméno koncového uživatele	Jméno koncového uživatele (pokud je uvedeno)	
IP adresa	IP adresy důvěryhodných zařízení, ze kterých koncoví uživatelé přistupovali ke službě LastPass	
Telefonní číslo	Číslo mobilního telefonu používané pro obnovení SMS (pokud je povoleno)	
Jedinečný identifikátor mobilního zařízení	Jedinečný identifikátor jakéhokoli mobilního zařízení používaného pro přístup ke službě LastPass	
Iterace PBKDF2 SHA256	Počet iterací PBKDF2, pro které byl koncový uživatel nakonfigurován	

Zákaznická databáze také obsahovala různé informace o oprávněních k účtu (např. Premium, Families, Teams atd.) a také položky konfigurace služeb a aplikací, jako jsou povolené možnosti MFA.

III. Data zákaznického trezoru LastPass

Aktér ohrožení dokázal zkopírovat pět fragmentů databáze Binary Large Objects (BLOB), které byly datovány: 20. srpna 2022, 30. srpna 2022, 31. srpna 2022, 8. září 2022 a 16. září 2022. místo mezi 8. a 22. zářím 2022. Účty LastPass vytvořené po těchto datech nejsou ovlivněny.

Anatomie "Vault"

Zákazníci by rozpoznali data „sejfu“ jako položky, jako jsou stránky a bezpečnostní poznámky a jejich různé dílčí prvky, se kterými interagují při používání klienta LastPass (webový prohlížeč, rozšíření, mobil atd.) na svém zařízení.

Agregovaná data úschovny jsou však ve skutečnosti sestavována z více zdrojů backendových dat a před sdílením s žádajícím klientem transformována/balena naší službou LastPass. Datové prvky zákaznického trezoru jsou uloženy v serializovaném datovém formátu popsaném jako BLOB sestávající z kolekcí binárních řetězců rozdělených do určených sekcí. Samotné struktury BLOB nejsou šifrovány jako celek, ale jsou v nich sekce/pole, která jsou šifrována.

Objekty BLOB, které jsou uloženy v backendu služby LastPass, přímo nepředstavují kompletní sestavené „sejfy“, které jsou vykresleny ve formě čitelné pro člověka v rámci klienta LastPass každého zákazníka. Místo toho backendová logika LastPass balí a transformuje prvky z objektů BLOB s daty uloženými v tomto binárním formátu, deserializuje je a kombinuje je s jinými daty z jiných zdrojů dat. Poté je přenesen na klienta a nakonec dekódován a dešifrován na straně klienta. Při aktualizaci objektů BLOB dochází k opačnému postupu.

Šifrovaná pole v trezoru

Šifrovaná datová pole v objektech BLOB jsou šifrována 256bitovým šifrováním AES. Dešifrování se provádí na lokálním klientovi LastPass koncového uživatele pomocí jedinečného šifrovacího klíče odvozeného z hlavního hesla každého uživatele. Vzhledem k naší architektuře Zero Knowledge nejsou hlavní hesla koncových uživatelů LastPass nikdy známa a LastPass je neukládá ani neuchovává. V objektech BLOB je 23 šifrovaných datových polí, z nichž 21 lze považovat za „citlivá“ data:

- V rámci Webů jsou šifrována následující pole:
  - Jméno stránky
  - Složka webu
  - Uživatelské jméno webu (včetně protokolu historie změn)
  - Heslo webu (včetně protokolu historie změn)
  - Obsah poznámky k webu (včetně protokolu historie změn)
  - Šifrovaný tajný klíč TOTP používaný ke generování kódů TOTP pro jednotlivé stránky
  - Vlastní vyplnitelné pole formuláře
  - Vlastní vyplnitelný obsah pole formuláře
- V rámci Secure Notes jsou šifrována následující pole:
  - název
  - Složka
  - Název souboru přílohy
  - Příloha
  - Šifrovaný klíč pro šifrování přílohy
  - Obsah poznámky

- Kromě toho jsou šifrována následující nekategorizovaná datová pole:
  - Názvy skupin
  - Šifrované klíče pro sdílení
  - Šifrovaný klíč sdílení Super Admin

Nešifrovaná pole v trezoru

V době psaní tohoto článku existuje 12 nešifrovaných datových polí, která mohou obsahovat citlivé informace, které odkazují na konkrétní uživatele nebo zařízení. Většina těchto položek je založena na URL nebo se týká URL a platí pouze v případě, že uživatel LastPass využívá určité specifické funkce, funkce nebo konfigurace účtu:

- Cesta k souboru aplikace pro aplikaci LastPass Windows nebo macOS
- E-mailová adresa uživatele LastPass, který upravuje sdílenou položku trezoru (zaznamenáno v historii změn)
- Adresy URL stránek, včetně různých pravidel pro adresy URL a konfigurací účtu „Nikdy URL“. Podrobnější seznam různých polí nešifrovaných adres URL naleznete níže:

	Název pole	Typ pole	Popis pole	Reference LastPass	Platí pro zákazníky/případy použití
1	*url*	URL	**URL** položky trezoru	Adresa URL webové stránky, kterou LastPass zachytí při uložení pověření a použije během vyplňování pověření pro spárování. Toto jsou plně kvalifikovaná doménová jména (FQDN) a sem lze přidat cokoli z adresy URL. Příklady: https://www.cnn.com nebo https://www.cnn.com/2023/01/09/sport/nfl-playoffs-set/index.html	Univerzálně dostupný pro **všechny zákazníky** , používaný všemi klienty při ukládání pověření do LastPass a používaný pro shodu URL/domény při vyplňování pověření.
2	*Rul*	URL	Duplikát pole URL	<Zastaralá funkce, ale duplikát #1>	Zastaralé, může existovat pro staré uživatele
3	*pravidla_url*	Seznam domén/URL	Při přihlašování k webu **zobrazí LastPass přihlašovací položky ve vašem trezoru s podobnou adresou URL.** Použijte pravidla URL k řízení tohoto procesu přiřazování a vytvoření plynulejšího prostředí.	Spravujte pravidla URL v Nastavení účtu	Univerzálně dostupné **všem zákazníkům** , ale konfigurované na vyžádání a existuje pouze v případě, že je tato funkce implementována.
4	*Equiv_domains*	Seznam domén/URL	Přidejte **domény** , které používají stejnou přihlašovací službu. Již jsme uvedli oblíbené weby, které používají sdílené přihlašovací údaje napříč doménami pod jejich kontrolou. Například:*amazon.com*a jeho lokální variace, popř*gmail.com*a další produkty Google	Spravujte ekvivalentní domény v nastavení účtu	Je univerzálně dostupný pro **všechny zákazníky** a LastPass konfiguruje některé vzorové domény ve výchozím nastavení, pokud je k tomu explicitně nakonfigurován. Toto jsou plně kvalifikovaná doménová jména (FQDN) a sem lze přidat cokoli z adresy URL.

	Název pole	Typ pole	Popis pole	Reference LastPass	Platí pro zákazníky/případy použití	
5	*accs_never*	Seznam adres URL	Používá se, když zákazníci deaktivují akce LastPass na **konkrétních webech/adresách URL (denylist)**	Spravujte adresy URL Never v Nastavení účtu	Univerzálně dostupné **všem zákazníkům** , ale konfigurované na vyžádání a existuje pouze v případě, že je tato možnost implementována. Toto jsou plně kvalifikovaná doménová jména (FQDN) a sem lze přidat cokoli z adresy URL.	
6	*accts_never_excluded*	Seznam adres URL	**Připojeno k #5 – toto je „seznam povolených“, který se překrývá s (denylist) v #5** Administrátoři LastPass Business mohou do administrátorské konzole přidat globální adresy URL nikdy a pouze globální adresy URL a řídit tak, zda chcete, aby LastPass vyzýval uživatele k akci. Kromě toho lze při přidávání globálních adres URL nikdy použít zástupný znak (*) pro subdoménu i podcestu.	Spravujte globální adresy URL nikdy a pouze globální adresy URL pro uživatele v nové administrátorské konzoli	Dostupné pro všechny **firemní** zákazníky, ale konfigurováno na vyžádání a existuje pouze v případě, že je tato možnost implementována pro pouze globální adresy URL.	
7	*acs*	URL	**Adresy URL pro aplikace jednotného přihlášení SAML používající starší službu jednotného přihlášení LastPass.** **Poznámka:** Toto je adresa URL poskytovatele služeb identifikující aplikaci třetí strany, do které se uživatelé přihlašují (např.*https://signin.aws.amazon.com/saml*)	Přihlaste se do aplikace SSO z vašeho trezoru LastPass	**Firemní uživatelé používající službu LastPass Legacy SSO** s aplikacemi přiřazenými administrátorem. Umožňuje uživateli přihlásit se k aplikaci jednotného přihlášení ze svého trezoru LastPass. Tyto adresy URL aplikací se zobrazují v klientovi LastPass v části „Aplikace přiřazené mně“ a jsou přednastaveny administrátory tak, aby umožňovaly přístup k publikovaným aplikacím jediným kliknutím SSO/SAML.	

	Název pole	Typ pole	Popis pole	Reference LastPass	Platí pro zákazníky/případy použití	
8	*launchurl*	URL	**Adresy URL pro aplikace jednotného přihlášení SAML používající starší službu jednotného přihlášení LastPass.** **Poznámka:** Může to být buď interní adresa URL LastPass (např.*https://lastpass.com/saml/launch/cfg/XXXXXX*), která výslovně neidentifikuje poskytovatele služeb nebo adresu URL poskytovatele služeb třetí strany (např.*https://signin.aws.amazon.com/saml*)	<Související s #7> Začátek místa, kde začíná relace ověřování SSO/SAML	**Firemní uživatelé používající službu LastPass Legacy SSO** s aplikacemi přiřazenými administrátorem. Umožňuje uživateli přihlásit se k aplikaci jednotného přihlášení ze svého trezoru LastPass. Tyto adresy URL aplikací se zobrazují v klientovi LastPass v části „Aplikace přiřazené mně“ a jsou přednastaveny administrátory tak, aby umožňovaly přístup k publikovaným aplikacím jediným kliknutím SSO/SAML.
9	*Appaccts – název aplikace*	Cesta aplikace	Cesta k aplikaci LastPass v souborovém systému Windows nebo macOS	Obsahuje cestu k nativní lokálně hostované aplikaci, pro kterou jste nastavili automatické vyplňování plochy	Univerzálně dostupné **všem zákazníkům,** ale konfigurované na vyžádání a existuje pouze v případě, že je tato funkce implementována pro použití nativní aplikace LastPass pro Windows nebo macOS. Nevztahuje se na případy použití webových stránek nebo rozšíření prohlížeče.	
10	*Accts_notes*	Emailová adresa	E-mailová adresa uživatele, který upravil pole poznámky položky trezoru	Používá se pro další historii změn – Zobrazení změn v historii položek	Univerzálně k dispozici **všem zákazníkům** , ale používá se pouze na vyžádání, když je sdílená položka aktualizována, někým, kdo není původním sdílejícím.	
11	*Accts_username*	Emailová adresa	E-mailová adresa uživatele, který upravil pole uživatelského jména položky úschovny	Používá se pro další historii změn – Zobrazení změn v historii položek	Univerzálně k dispozici **všem zákazníkům** , ale používá se pouze na vyžádání, když je sdílená položka aktualizována, někým, kdo není původním sdílejícím.	
12	*Accts_password*	Emailová adresa	E-mailová adresa uživatele, který upravil pole hesla položky trezoru	Používá se pro další historii změn – Zobrazení změn v historii položek	Univerzálně k dispozici **všem zákazníkům** , ale používá se pouze na vyžádání, když je sdílená položka aktualizována, někým, kdo není původním sdílejícím.	

Bulletiny zákaznické bezpečnosti

Aktér ohrožení se může pokusit o hrubou sílu a dešifrování kopií dat z trezoru, které pořídil. Naše šifrovací architektura Zero Knowledge je navržena tak, aby chránila citlivé informace zákazníků a bránila se tak pokusům o hrubou sílu zašifrovaných dat. Aktér ohrožení může také použít některá z těchto dat k cílení na zákazníky pomocí phishingových útoků, vycpávání přihlašovacích údajů nebo jiných útoků sociálního inženýrství proti online účtům spojeným s jejich trezorem LastPass.

Abychom našim zákazníkům lépe pomohli s řízením těchto rizik, připravili jsme dva bulletiny zabezpečení – jeden pro naše spotřebitelské uživatele Free, Premium a Families a jeden přizpůsobený našim uživatelům Business a Teams:

- **Bulletin zabezpečení: Doporučené akce pro bezplatné, prémiové a rodinné zákazníky .** Tento bulletin provede naše zákazníky Free, Premium a Families kontrolou důležitých nastavení LastPass navržených tak, aby pomohly zabezpečit jejich účet potvrzením dodržování osvědčených postupů.
- **Bulletin zabezpečení: Doporučené akce pro podnikové administrátory LastPass .** Tento bulletin provede administrátory našich zákazníků Business a Teams posouzením konfigurace účtu LastPass a integrací třetích stran a obsahuje informace, které jsou relevantní pro nefederované i federované zákazníky.

Máte-li jakékoli dotazy týkající se doporučených akcí, kontaktujte prosím technickou podporu nebo tým pro úspěch zákazníků, kteří jsou připraveni vám pomoci.