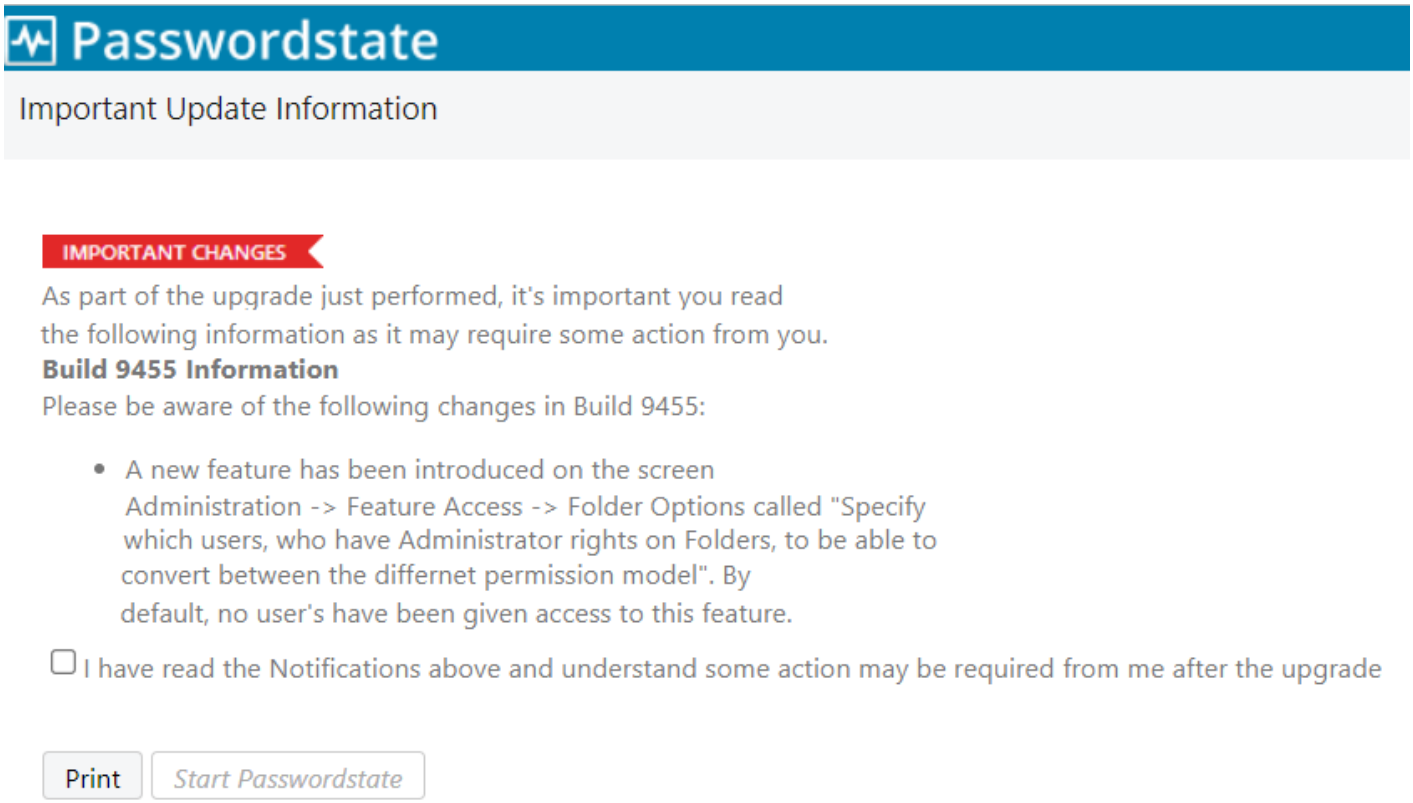
CVE-2022-25570: Standard Berechtigungsmodell im Passwortmanager Passwordstate ermöglicht Rechteausweitung

von Benjamin Pokrantam 2022-03-18 in Passwordstate



Für die Verwaltung der zahlreichen Kennwörter nutzen viele Anwender einen Passwortmanager und folgen damit beispielsweise auch der Empfehlung des BSI. Bei dem Passwortmanager Passwordstate vom Hersteller Click Studios (SA) Pty Ltd haben die System Engineers der fibcom GmbH Auffälligkeiten im Standard Ordner-

Berechtigungsmodell entdeckt. Das gezeigte Verhalten ermöglicht es, einem authentifizierten Benutzer, welcher über Schreibberechtigungen für eine Passwortliste in einem Ordner verfügt, seine Berechtigungen auf alle weiteren Passwortlisten im gleichen Ordner auszuweiten.

Die System Engineers informierten den Hersteller deswegen über das beobachtete Verhalten der Software. Click Studios (SA) Pty Ltd hat nach dem Eingang des Hinweises innerhalb kürzester Zeit die Version 9455 mit einem angepassten Berechtigungsmodell veröffentlicht. Die Entwickler haben wie gewohnt sehr schnell reagiert und das Problem behoben. Administratoren von Passwordstate sollten die neue Version dementsprechend schnellstmöglich installieren.

Kommunikation mit Click Studios (SA) Pty Ltd

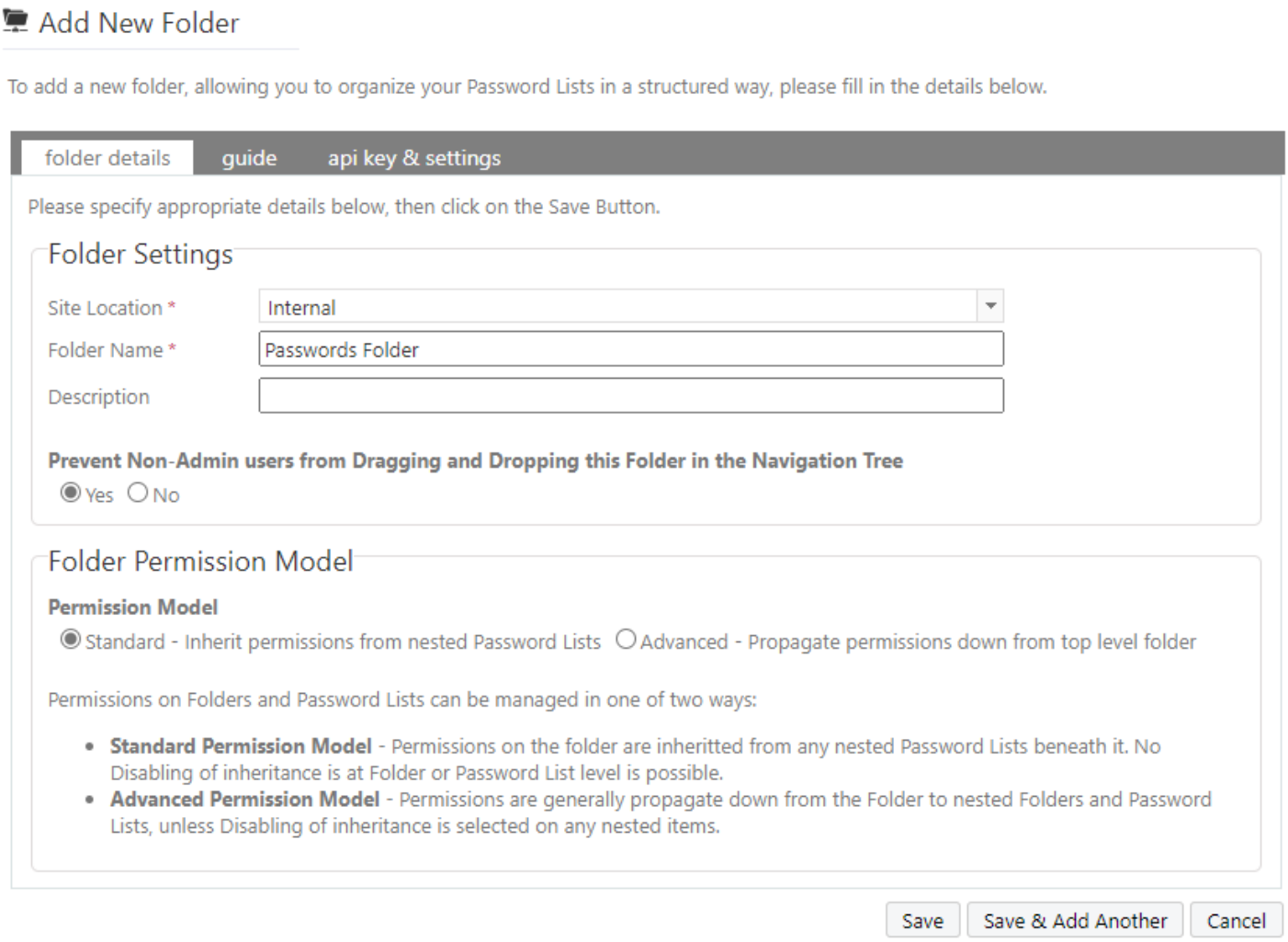
Anfänglich noch vom äußerst professionellen Support beantwortete Fragen unsererseits übernahm dann bald der zuständige General Manager. Er erklärte, dass Click Studios (SA) Pty Ltd das gezeigte Verhalten **nicht** als eine Schwachstelle sehe. Click Studios (SA) Pty Ltd betonte gegenüber den System Engineers der fibcom GmbH, dass man für Fehlkonfigurationen keine Verantwortung übernehme und erklärte, dass das Testsetup eine solche Fehlkonfiguration ausnutze. Weiterhin beschrieb Click Studios (SA) Pty Ltd eine hohe Komplexität ihrer Software, welche mit der großen Flexibilität der Software einher gehe. Passwordstate könne daher nicht von durchschnittlichen Benutzern administriert werden, sondern erfordere einen disziplinierten Verwaltungsansatz.

Aus unserer Sicht stellt das beobachtete Verhalten, welches schon in der Standardkonfiguration auftritt, klar eine Schwachstelle dar. In einem so schützenwerten Asset wie einem Passwortmanager sehen wir eine Rechteausweitung als besonders kritisch und schätzen den Umgang mit unserer Meldung daher als schwierig ein. Da seitens Click Studios (SA) Pty Ltd eine Einstufung als Schwachstelle vermieden wird und damit Administratoren die Dringlichkeit eines Updates unter Umständen verborgen bleibt, soll dieser Beitrag dabei helfen jedem Leser eine eigene Einschätzung der Sachlage zu ermöglichen.

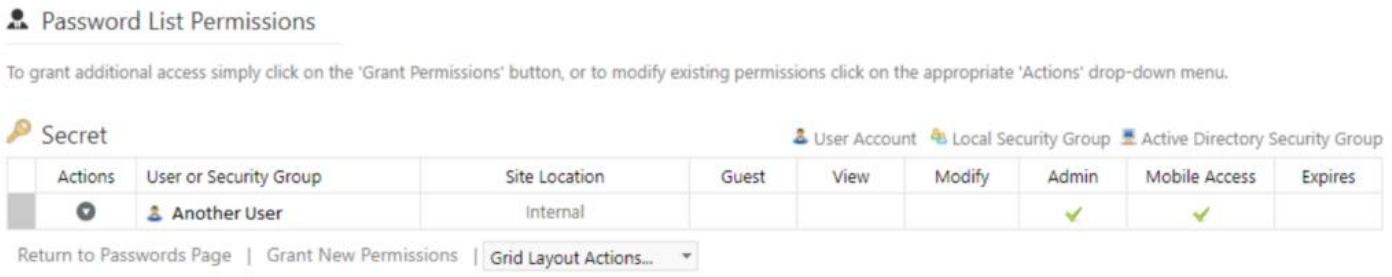
Vorgehensweise

Um das Verhalten nachzustellen, können Passwortstate Benutzer folgende Schritte ausführen:

1. Erstellen eines Ordners „Passwords Folder“ mit dem Berechtigungsmodell **Standard**.



2. Erstellen einer Shared Password List „Secret“ in „Passwords Folder“ mit einem Beispielpasswort.
3. Erstellen einer Shared Password List „Public“ in „Passwords Folder“.
4. Zuweisen von Schreibberechtigungen auf die Passwortliste „Public“ für den Benutzer „Mallory“.
5. Anschließend feststellen, dass Mallory keine Berechtigungen für die Passwortliste „Secret“ besitzt.

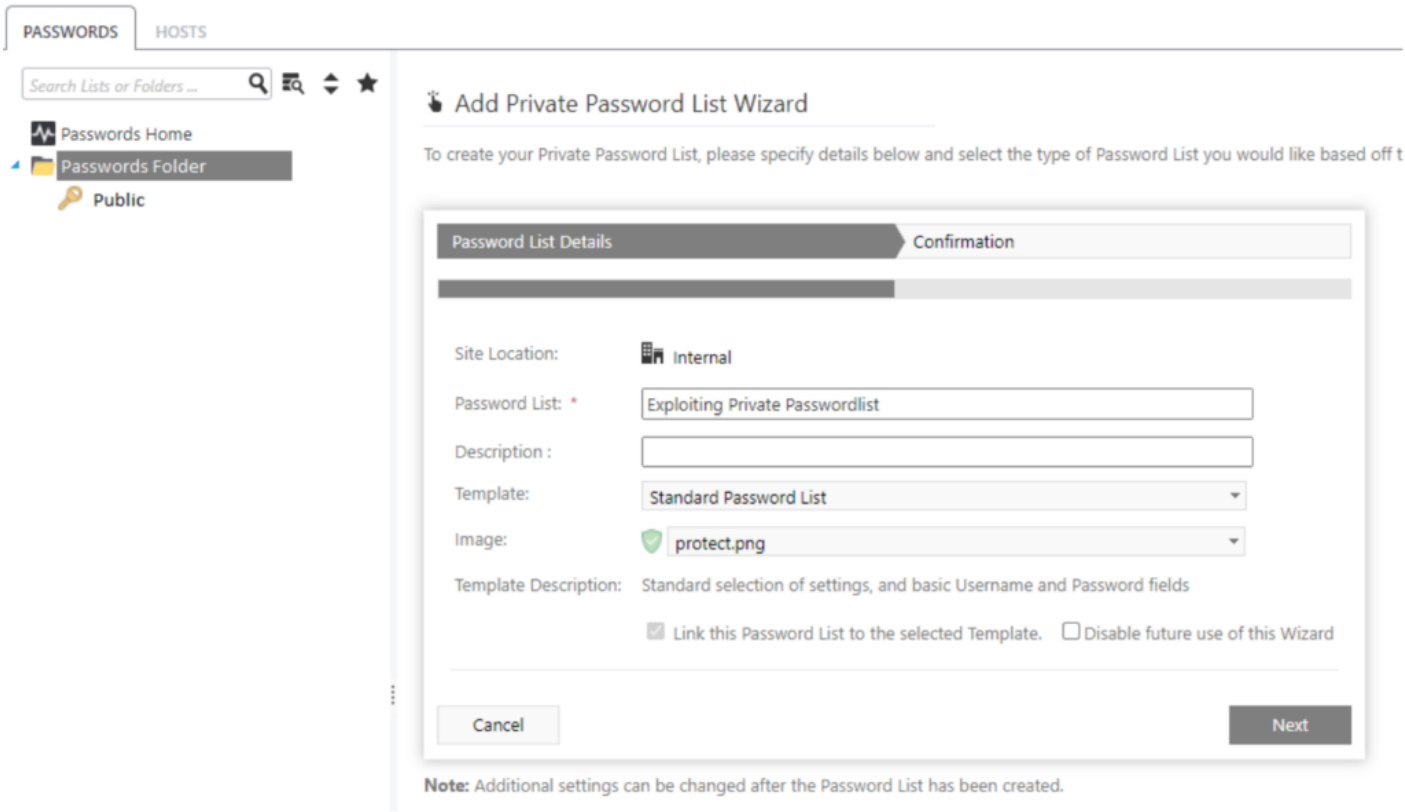


6. Beim Berechtigungsmodell **Standard** setzt Passwortstate die Berechtigungen für das Ordnerobjekt aus den untergeordneten Berechtigungen der Passwortlisten zusammen. Deshalb zeigt die Berechtigung auf dem Ordner Admin Berechtigungen für „Another User“ und „Modify“ Berechtigungen für Mallory

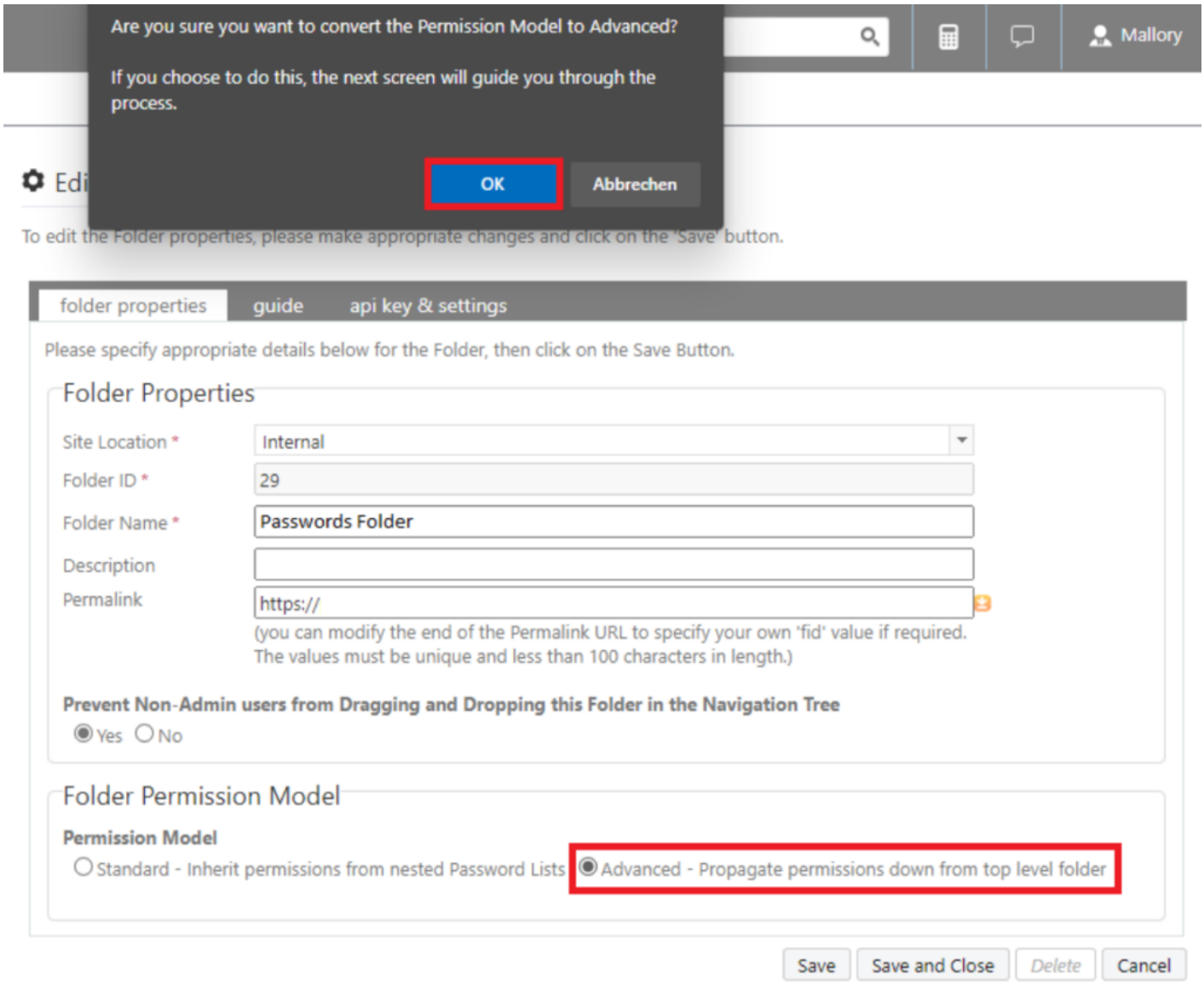
Actions	User or Security Group	Site Location	Guest	View	Modify	Admin	Expires
	Another User	Internal				✓	
	Mallory	Internal			✓		

Return to Password Folder | Grant New Permissions | Grid Layout Actions...

7. Dann als Mallory angemeldet eine Private Password List im Ordner „Passwords Folder“ anlegen. Der Screenshot zeigt nochmals, dass Mallory nur die Passwortliste „Public“ sehen kann.



8. Weiterhin als Mallory angemeldet einen Rechtsklick auf „Passwords Folder“ ausführen und „Edit Properties“ auswählen.
9. Im Folgenden kann Mallory das Berechtigungsmodell von **Standard** auf **Advanced** ändern.



10. Feststellen, dass Mallory nun in den Berechtigungen des Ordners zusätzlich als „Admin“ aufgeführt wird und damit folgerichtig Zugriff auf sämtliche Passwortlisten des Ordners hat.

Diskussion

An dieser Stelle sei darauf hingewiesen, dass keine besondere Konfiguration in Passwordstate vorgenommen wurde. Das gezeigte Verhalten tritt also in der Standardeinstellung auf. Aus Sicht der System Engineers ist es

einem Administrator nicht möglich, diese Auswirkungen bei der Verwendung des Standard Berechtigungsmodells zu erkennen. Click Studios (SA) Pty Ltd brachte ein, dass das Verhalten durch das Deaktivieren eines Hakens bei „Modify“ in den Einstellungen hätte verhindert werden können.

Tatsächlich kann ein Nutzer dann keine Passwortlisten mehr in Ordnern erstellen und dadurch dann auch nicht mehr seine Rechte innerhalb eines Verzeichnisses erweitern. Jedoch schränkt diese Einstellung die Funktion von Passwordstate auch erheblich ein und erlaubt Nutzern keine eigenen Passwortlisten in allen Ordnern. Dies gilt dann auch für das Advanced Berechtigungsmodell. Zudem geht aus der Einstellung nicht hervor, dass das Erstellen neuer Passwortlisten solche Auswirkungen auf das Berechtigungsmodell sowie andere Passwortlisten hat.

Berechtigungsmodell in Version 9455 korrigiert

Obwohl es dem Hersteller nach keine Schwachstelle sei, hat das Team von Click Studios (SA) Pty Ltd das Berechtigungsmodell **Standard** mit der neuen Version abgesichert. Durch die Verbesserung können nur noch explizit über eine neue Einstellung berechtigte Benutzer das Berechtigungsmodell von Ordnern ändern, wobei standardmäßig kein Benutzer über diese Berechtigung verfügt.

Nach der Installation des Updates können Benutzer schließlich sowohl in neuen als auch in bestehenden Installationen ihre Rechte nicht mehr auf die beschriebene Weise ausweiten. Sollen Benutzer weiterhin das Berichtigungsmodell von Ordnern ändern können, müssen Administratoren also die beschriebene Einstellung vornehmen. Jedoch wurde durch Click Studios (SA) Pty Ltd darauf hingewiesen, dass diese Absicherung keine Fehlerbehebung sei, sondern nur ein kleineres Update und die schnelle Reaktion nur Zufall. Bei der Installation des Updates wird trotzdem ein großer Hinweis zu diesem „minor update“ angezeigt:

Das in Passwordstate beobachtete Verhalten wird aufgrund des in diesem Beitrag beschriebenen Verhaltens von uns als Schwachstelle betrachtet. Mit Click Studios (SA) Pty Ltd konnte hierüber keine Einigung erzielt werden. Mehrfache Gesprächsangebote wurden ignoriert. Abschließend wird festgestellt, dass wohl verschiedene Perspektiven auf den Sachverhalt existieren.

Schwachstellenbewertung nach CVSS

Durch das gezeigte Verhalten können, je nachdem wie die Verzeichnisstruktur in Passwortstate aufgebaut ist, erhebliche Einschränkungen der Sicherheit entstehen. Benutzer können möglicherweise an zusätzliche Berechtigungen mit höchsten Privilegien gelangen. Falls dies also eine Schwachstelle ist, könnte die nachfolgende Bewertung angewendet werden.

Gesamtbewertung: 9,9

Impact

- Confidentiality: High
- Integrity: High
- Availability: High

Exploitability

- Access Vector: Network
- Access Complexity: Low
- Privileges Required: Low
- User Interaction: None

Scope

- Scope: Changed

Zeitlicher Ablauf

- 2022-02-17 Erste Kontaktaufnahme mit dem Hersteller
- 2022-02-17 Erste Reaktion des Herstellers
- 2022-02-18 Detaillierte Meldung an den Hersteller
- 2022-02-22 Veröffentlichung Version 9455 mit angepasstem Berechtigungsmodell
- 2022-03-17 Veröffentlichung des Fundes als Blogbeitrag

Vorheriger Artikel
KeePass Alternative Passwordstate von Clickstudios

Veröffentlicht unter Passwordstate
Markiert in Clickstudios, Kennwortverwaltung, Passwordmanagement, Passwordstate

Suche

Folgt uns auf:

Kategorien

- Active Directory
- AeroHive
- Linux

- Monitoring
- Netzwerk
- Nextcloud
- Passwordstate
- pfSense
- PowerShell
- Snort
- VPN
- Windows Sever

Tags

802.1X @click_studios APU2C4 arubanetworks Automation clearpass Clickstudios ClientVPN Cluster DHCPPool dnssec DynamicDNS DynDNS Firewall Gateway GoDaddy HighAvailability hpe IDS IPS IPSec KeePass Kennwortverwaltung Microsoft nac NAT Netgate NetworkAccessControl NetworkAddressTranslation Networking Netzwerk OpenAppID Passwordstate Passwortverwaltung PCEngines pfSense PowerShell Server2016 ServerCore Site2Site Snort VPN Windows WindowsAdminCenter WLAN

Copyright © 2022 SysAdm's Blog. Alle Rechte vorbehalten.