Rollout 528

Inhaltsverzeichnis

- 1 TeamDavid Client
- 2 TeamDavid PostMan
- 3 TeamDavid Client Mac
- 4 TeamDavid WebBox
- 5 TeamDavid Service Layer

Release Notes zu Rollout 528 vom 30.06.2026

1 TeamDavid Client

Das aktuelle Update umfasst mehrere Neuerungen: Die Spaltenbreiten der Liste der Anhänge in der Vorschau werden nun gespeichert und bei jedem Start wiederhergestellt. Zudem wurde ein neuer Button im Kalendereditor hinzugefügt, der es ermöglicht, eine E-Mail an alle Teilnehmer eines Kalendereintrags zu senden. Abschließend wird bei der Erstellung des WebView Cache Pfades in RDP-Sitzungen sichergestellt, dass Leerzeichen im Rechnernamen entfernt werden. Alle Änderungen sind Teil des #TeamClient.

Übersicht der Anpassungen:

- Speichern der Spaltenbreiten bei Dateianhängen
  Die Spaltenbreite der Liste der Anhänge in der Vorschau wird nach manueller Veränderung nun gespeichert und beim Start wiederhergestellt.
- Info an Teilnehmer einer Besprechung senden
  Wird ein Kalendereintrag mit mehreren Teilnehmern geöffnet, kann nun über den neuen Button „Info an Teilnehmer“ eine eMail an alle Teilnehmer gesendet werden.
- Erstellung des WebView Cache Ordners ohne Leerzeichen
  Bei der Erstellung des Cache Pfades der WebView wird u.a. in RDP Sitzungen der Rechnername verwendet. Enthält dieser Leerzeichen, werden diese nun entfernt.

Quelle: Tobit

2 TeamDavid PostMan

Im aktuellen Update wurden mehrere Verbesserungen implementiert. Die eMail-Authentifizierung per DKIM kann jetzt für autorisierte Absender optimiert werden, wodurch verhindert wird, dass deren E-Mails fälschlicherweise als SPAM eingestuft werden. Zudem wurde die MTA-STS-Zertifikatsprüfung so angepasst, dass der Domainname für die Server-Zertifikatsabfrage immer in Kleinbuchstaben verwendet wird, um Validierungsfehler zu vermeiden. Weitere Details sind im Zusammenhang mit #TeamDavidPostMan zu finden.

Übersicht der Anpassungen:

- Autorisierte Absender von der DKIM-Spam-Erkennung ausschließen
  Ist im PostMan die eMail-Authentifizierung per DKIM aktiviert, so kann dies für bestimmte Absender unterbunden werden, wenn diese im PostMan unter Datenbanken/Erlaubte Absenderadressen eingetragen werden.

- Optimierung bei MTA-STS-Zertifikatsprüfung
  Bei der MTA-STS-Zertifikatsprüfung wird nun sichergestellt dass der Domainname für die Server-Zertifikatsabfrage immer in Kleinbuchstaben vorliegt, um mögliche Validierungsfehler aufgrund von Groß-/Kleinschreibung zu vermeiden.

Quelle: Tobit

3 TeamDavid Client Mac

Die aktuelle Version umfasst mehrere Optimierungen und neue Features, darunter eine verbesserte Suche in der InfoCenter Ansicht und eine optimierte Hyperlink-Verwaltung im Editor. Zudem können Markierungen in der Nachrichtenliste jetzt direkt über das Kontextmenü gesetzt werden. Die Anzeige der Kontaktbilder wurde für verschiedene Accounts optimiert, und die Badge-Anzeige in der Favoritenleiste wurde ebenfalls verbessert. Weitere Anpassungen betreffen das Drag & Drop sowie die Darstellung von Symbolen und Aufgaben. Diese Änderungen stärken die Benutzererfahrung und verbessern die Funktionalität im #TeamDavidmacOS.

Übersicht der Anpassungen:

- Optimierung der Suche in InfoCenter Ansicht
  Die Suche in der InfoCenter Ansicht wurde optimiert.
- Optimierung beim Einfügen von Hyperlinks
  Das Einfügen von Hyperlinks im Editor wurde optimiert.
- Markierungen setzen in der Nachrichtenliste
  In der Nachrichtenliste können Markierungen jetzt direkt über das Kontextmenü gesetzt oder entfernt werden.
- Optimierung bei Anzeige der Kontaktbilder
  Die Anzeige der Kontaktbilder bei eMails wurde optimiert - vor allem bei der Verwendung von verschiedenen Accounts und Servern.
- Optimierung der Badge Anzeige in Favoritenleiste
  Die Badge Anzeige in der Favoritenleiste wurde optimiert.
- Mögliches Fehlverhalten beim Drag & Drop von Nachrichten
  In Einzelfällen was das Verschieben/Kopieren von Nachrichten aus bestimmten Ordnern nicht möglich.

Quelle: Tobit

4 TeamDavid WebBox

Die aktuelle Version beinhaltet eine Aktualisierung der openssl Version, wobei die Datei davidtls.dll nun auf openssl 3.6 basiert. Zudem wurde der alte David Client Web (Web-Access) deaktiviert; dies geschieht nun standardmäßig über einen neuen Schalter in der WebBox Konfiguration. Bei Aufruf der bisherigen Startseite des Web-Access erfolgt eine automatische Umleitung auf https://tobit.team. #TeamDavidWebBox

Übersicht der Anpassungen:

- Aktualisierung der openssl Version
  Die davidtls.dll wurde auf openssl 3.6. aktualisiert.
- Deaktivierung des alten David Client Web (Web-Access)
  Der alte Web-Access wird nun durch einen neuen Schalter in der WebBox Konfiguration per Vorgabe deaktiviert. Beim Aufruf der bisherigen Startseite des Web-Access wird automatisch auf die Seite https://tobit.team umgeleitet.

Sicherheitshinweis / CVEs

Im Zusammenhang mit dem bisherigen David Client Web (Web-Access) wurden uns verschiedene Sicherheitsschwachstellen gemeldet, die inzwischen als CVEs veröffentlicht wurden.

Ein Teil der gemeldeten Schwachstellen wurde bereits mit vorherigen Rollouts durch entsprechende Anpassungen behoben. Unabhängig davon haben wir uns dazu entschieden, die betroffene Web-Access-Funktionalität nicht weiterzuführen.

Mit Rollout 528 wurde die betroffene Funktionalität standardmäßig deaktiviert. Die entsprechende Schnittstelle wurde abgekündigt und wird nicht weiterentwickelt.

Damit ist die von den nachfolgend aufgeführten CVEs betroffene Funktionalität ab Rollout 528 standardmäßig nicht mehr aktiv:

- CVE-2026-12070 – Arbitrary File Deletion
- CVE-2026-12071 – Header Injection leading to Open Redirect
- CVE-2026-54199 – Header Injection
- CVE-2026-54200 – Local File Inclusion
- CVE-2026-54201 – Missing Authorization
- CVE-2026-54202 – Path Traversal
- CVE-2026-54203 – Memory Leak / Sensitive Information Disclosure
- CVE-2026-54204 – Server-Side Request Forgery (SSRF)
- CVE-2026-54205 – Server-Side Request Forgery (SSRF)
- CVE-2026-54206 – Server-Side Request Forgery (SSRF)
- CVE-2026-54207 – Server-Side Request Forgery (SSRF)
- CVE-2026-54208 – Arbitrary File Write leading to Stored XSS
- CVE-2026-54209 – Buffer Overflow in editini
- CVE-2026-54210 – Buffer Overflow in File Names
- CVE-2026-54211 – Buffer Overflow in Form Data
- CVE-2026-54212 – Buffer Overflow in JSON Parsing
- CVE-2026-54213 – Denial of Service
- CVE-2026-54214 – Header Injection
- CVE-2026-54215 – Open Redirect
- CVE-2026-54216 – Reflected Cross-Site Scripting (XSS)
- CVE-2026-54217 – Stored Cross-Site Scripting (XSS)
- CVE-2026-54218 – Weak Cryptography and Insecure Password Storage

Die Auflistung entspricht den 22 veröffentlichten CVEs zu diesem Thema.

Wir empfehlen allen Kunden, mindestens Rollout 528 oder eine neuere Version von TeamDavid einzusetzen.

Quelle: Tobit

5 TeamDavid Service Layer

Im aktuellen Update des David Administrators wurde die Möglichkeit hinzugefügt, das „Model Context Protocol“ (MCP) in der WebAPI Konfiguration zu aktivieren, was sich derzeit in der Beta-Phase befindet. Anwender können nun ihre Daten, wie eMails und Termine, analysieren, sofern ein SideKick Server eingerichtet ist. Zudem wurde die Funktionalität erweitert, einen eigenen Agenten unter „Intelligent Agents“ hinzuzufügen und eine externe Verbindung über das MCP einzurichten. #TeamDavidServiceLayer

Übersicht der Anpassungen:

- Im David Administrator kann nun in der WebAPI Konfiguration das „Model Context Protocol“ (MCP) aktiviert werden (bisher noch Beta). Ist ein SideKick Server eingerichtet, kann der David Anwender somit seine Daten (z.B. eMails, Termine) analysieren lassen. Hierzu wird beim SideKick Server unter „Einstellungen/chayns OS Konfiguration/Verbindungen/SideKick“ ein MCP Eintrag hinzugefügt mit der URL der WebAPI (z.B. https://webapi-site:8443/mcp). Unter „Intelligent Agents“ kann nun ein eigener Agent hinzugefügt und benannt werden. Unter „Erweitert“ kann anschließend die „Externe Verbindung (MCP)“ eingerichtet und verbunden werden.

Quelle: Tobit