Baden-Württemberg

LANDESKRIMINALAMT

Warnmeldung für Firmen und Behörden

Sensible VPN-Benutzerdaten von Kunden des Herstellers Fortinet im Internet veröffentlicht

Stuttgart, 10. September 2021

Im Internet ist eine Liste ausgespähter Benutzerkonten für den Fernzugriffsdienst Fortinet VPN veröffentlicht worden. Die Liste enthält die vollständigen Zugangsdaten für mehrere Tausend Benutzerkonten. Darunter befinden sich mehr als 2.000 Benutzerkonten, die Anwendern und Anwenderinnen in Deutschland zugeordnet werden.

Bei dem betroffenen Dienst „FortiGate SSL-VPN“ handelt es sich um eine Anwendung, die überwiegend bei Firmen zum Einsatz kommt und beispielsweise im Homeoffice oder von externen IT-Servicedienstleistern für den Zugriff auf das Netzwerk genutzt wird.

Die ausgespähten und im Internet veröffentlichten Zugangsdaten können zum unberechtigten Zugriff auf das IT-Netzwerk der betroffenen Betriebe verwendet werden. Unberechtigte können auf im Netzwerk gespeicherte Daten zugreifen, Daten ausspähen und Daten sabotieren.

Die Zugangsdaten wurden in der Vergangenheit vermutlich über eine Sicherheitslücke (CVE-2018-13379) des Forti-Betriebssystems ausgespäht. Betroffen von der Sicherheitslücke waren folgende Softwareversionen:

- FortiOS 6.0 - 6.0.0 to 6.0.4
- FortiOS 5.6 - 5.6.3 to 5.6.7
- FortiOS 5.4 - 5.4.6 to 5.4.12

Hierzu veröffentlichte der Hersteller bereits ein Update, das diese Sicherheitslücke beseitigt. Auch nach dem Einspielen der Sicherheitsupdates können zuvor unerlaubt erlangte Zugangsdaten zum unberechtigten Netzwerkzugriff verwendet werden.

Sofern zu irgendeinem Zeitpunkt die o.g. Softwareversionen bei Ihnen im Einsatz waren, empfehlen wir daher die zeitnahe Umsetzung folgender Maßnahmen:

- Deaktivieren Sie alle VPN-Verbindungen des Dienstes.
- Prüfen Sie eventuell unberechtigt eingerichtete Netzwerkverbindungen (abweichendes Verhalten, atypische IP-Adressen und Zugriffszeiten, ungewöhnliche Datentransfers).
- Installieren Sie die vom Hersteller Fortinet zur Verfügung gestellten Updates und Upgrades.
- Setzen Sie alle Benutzerkonten zurück.
- Prüfen Sie, ob die verwendeten Passwörter auch für andere Dienste genutzt worden sind und leiten gegebenenfalls Gegenmaßnahmen ein und informieren die Anwenderinnen und Anwender, Passwörter niemals mehrfach zu verwenden.
- Veranlassen Sie die globale Neuvergabe der Zugangspasswörter.
- Verhindern Sie mit geeigneten technischen Mitteln, dass die Anwenderinnen und Anwender alte Passwörter wiederverwenden.
- Aktivieren Sie die Absicherung der VPN-Benutzerkonten mit einem „Zweiten Sicherheitsfaktor“.

Weitere Informationen und Handlungsempfehlungen können Sie den folgenden Webseiten entnehmen:

- https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials
- https://www.fortiguard.com/psirt/FG-IR-18-384

Allgemeine Empfehlungen der Polizei:

- Prüfen Sie regelmäßig, ob die von Ihnen verwendeten Systeme und Softwareprodukte von den Herstellern noch unterstützt werden und installieren Sie zeitnah bereitgestellte Updates.

Stellen Sie unberechtigte Zugriffe auf das Netzwerk Ihrer Institution fest, können Sie sich an die Zentrale Ansprechstelle Cybercrime (ZAC) für Wirtschaftsunternehmen und Behörden in Baden-Württemberg wenden.

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg

Die ZAC dient als zentraler Ansprechpartner für die Wirtschaft und Behörden in allen Belangen des Themenfeldes Cybercrime.

Erreichbarkeit der ZAC:

Telefon: +49 (0)711 5401 2444

E-Mail: **cybercrime@polizei.bwl.de**

Website: www.lka-bw.de/zac