it.sec Research Team findet unbekannte Schwachstelle in Persis Online Bewerberportal

21. Januar 2021

Im Zuge eines Kundenprojekts konnte das Research Team der it.sec GmbH eine bisher unbekannte Schwachstelle im Persis Online Bewerberportal identifizieren und ausnutzen. Hierbei handelte es sich um die Manipulation eines Requests, welcher zur Weiterempfehlung von Stellenausschreibungen verwendet wurde. Die Schwachstelle wurde als Cross Site Scripting (XSS) deklariert.

Das Formular zur Weiterempfehlung von Stellenausschreibungen konnte verwendet werden, um Spammails zu versenden. Die eingesetzte Captcha-Funktion konnte das automatisierte und somit massenhafte Versenden von Spammails auf den ersten Blick verhindern. Dennoch konnte die Funktion genutzt werden, um eigene Nachrichten mit nahezu beliebigem Inhalt zu versenden. Somit könnte unter Umständen eine Vielzahl von Spammails im Namen des Kunden versendet werden. Folglich könnte die verwendete Domain auf einer Spam-Mailliste landen, wodurch die Mitarbeiter der Firma vermutlich keine Mails mehr an Kunden aussenden bzw. empfangen könnten.

Der Parameter „ABSENDER" im POST-Request konnte verwendet werden, um HTML einzufügen und somit die Nachricht zu manipulieren. Die Nachrichten wurden dann von noreply@domain.TLD versandt, wobei der Betreff nicht angepasst werden konnte.

Die Schwachstelle wurde vom it.sec Research Team an die Persis GmbH gemeldet und umgehend in den nächsten Releases behoben. Ein Workaround steht ebenso bereit.

Betroffenes Produkt: Online Bewerberportal mit Stellenausschreibung weiterempfehlen

Betroffene Version(en): 17.2.00 – 17.2.35 und 19.0.00 – 19.0.20

Betriebssystem: Linux, Windows

Behobene Version(en): 17.2.36, 19.0.21

Workaround ohne Update (QuickFix): Funktion „Stellenausschreibung weiterempfehlen" in den Einstellungen deaktivieren und durch einfache Browserfunktionalität (teilen) ersetzen

Ansprechpartner beim Hersteller:

Persis GmbH

Michael Barth

Geschäftsführer

E-Mail kontakt@persis.de

https://www.persis.de/

Die Schwachstelle (CVE-2020-35753) wurde bereits behoben und ein Security Patch steht für den Administrator innerhalb der Anwendung Persis zum Download zur Verfügung. Produktverantwortliche wurden über die Applikation benachrichtigt. Wir raten allen Betreibern Sicherheitsupdates stets zeitnah zu installieren, um bekannte Schwachstellen zu beheben.

Ihr it.sec Research Team

Bewerberportal | Captcha-Funktion | Cross Site Scripting | CVE-2020-35753 | Manipulation eines Requests | Persis Online | Research Team | Schwachstelle | Spammails | Weiterempfehlung von Stellenausschreibungen | XSS