Sicherheitslücken im Dedoles-Shop

Es gibt Unternehmen, die vorbildlich auf die ihnen gemeldeten Sicherheitslücken reagieren – und es gibt den Bekleidungsshop Dedoles. Der Shop wurde vor Monaten über XSS-Anfälligkeiten informiert, hat sich bisher jedoch nicht gerührt.

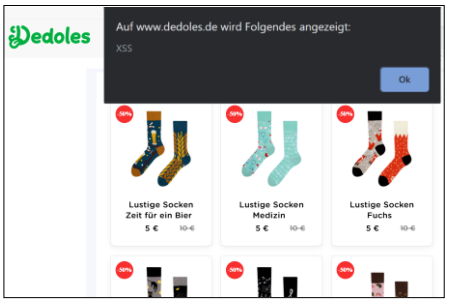
In der Vorweihnachtszeit haben Onlineshops Hochkonjunktur und auch der Corona-Lockdown kurz vor Weihnachten dürfte den virtuellen Geschäften weiteren Zulauf beschert haben. Doch auch wer sich den Innenstädten ferngehalten und auf der heimischen Couch geshoppt hat, war unter Umständen einem Risiko ausgesetzt: Der Bekleidungsshop Dedoles hat Sicherheitslücken auf seiner Website über Monate nicht gestopft.

Dedoles verkauft vor allem lustige Socken, Höschen und Boxershorts. Und das sehr erfolgreich, schenkt man den Unternehmensangaben Glauben: Demnach haben bereits über eine Million Kunden bei Dedoles bestellt, die slowakische Firma ist in 19 Ländern Europas aktiv, auch in Deutschland. Der Sicherheitsexperte Daniel Ruf interessierte sich jedoch nicht für die bunten Socken, sondern für die IT-Sicherheit des Shops. Ruf entdeckte prompt mehrere Schwachstellen des Typs „Cross Site Scripting“ (XSS) im Shopsystem. Lange suchen musste er dafür nicht: Die erste fand er gleich auf der Startseite, in einer zentralen Funktion des Shops.

XSS-Lücken zählen zu den häufigsten Sicherheitsproblemen von Websites. Patzt ein Server bei der Überprüfung von Nutzereingaben, zum Beispiel bei eingetippten Suchbegriffen, dann bekommt ein Angreifer die Chance, eigenen Code in die Website einzuschleusen. Dieser wird dann vom Browser des Opfers im Kontext der Site ausgeführt. Der Angreifer kann so zum Beispiel Zahlungsdaten ausleiten oder Schadsoftware verteilen.

Solche Lücken sind zwar gefährlich, aber auch leicht zu beheben. Es sind nur kleine Änderungen am Quellcode nötig, um potenziell gefährliche Zeichen aus Nutzereingaben herauszufiltern und das Einschleusen von schädlichen Inhalten effektiv zu verhindern. Daniel Ruf hatte Dedoles pflichtbewusst über seine Funde informiert, in der Hoffnung, dass die Lücken geschlossen werden, bevor sie von Cyber-Schurken entdeckt werden. Doch passiert ist nichts: „Bislang gab es keinerlei Antwort oder Reaktion von Dedoles auf meine Nachrichten“, erklärte er gegenüber c’t. Er bat uns deshalb, den Fall zu übernehmen.

Wir suchten daraufhin nach einem geeigneten Ansprechpartner bei dem Socken-Shop und kontaktierten am 20. Oktober die Pressestelle des Unternehmens.



Lustige Socken, löchriger Shop: Dedoles hat seit Monaten Probleme mit XSS-Lücken.

In unserer Mail befanden sich nicht nur sämtliche Informationen, die zur Behebung der Schwachstellen nötig sind, sondern auch einige Standardfragen: Wie lange existieren die Sicherheitslücken schon, wurden sie bereits von Cyber-Schurken genutzt und so weiter. Das Unternehmen reagierte auch auf unsere Mail nicht. Rund einen Monat später, am 16. November, kontaktierten wir Dedoles erneut. Auch dieses Mal warteten wir einen Monat auf eine Antwort – vergebens. Unsere Fragen blieben unbeantwortet, die Lücken ungepatcht. *(rei@ct.de)*

Ihr Hinweis an heise Investigativ:
https://heise.de/investigativ