Untis GmbH
Belvederegasse 11
A-2000 Stockerau

T: +43 (0) 2266/62241-0
E: office@untis.at
www.untis.at

Sehr geehrte WebUntis Administratoren,

wir möchten Sie darauf hinweisen, dass wir mit der WebUntis Version 2020.9.6 zwei Sicherheitslücken geschlossen haben:

Cross-Site-Request-Forgery
Unter bestimmten Umständen war es möglich, gefälschte WebUntis Nachrichten zu schicken. Folgende Vorbedingungen mussten dabei erfüllt sein:

- Aktive WebUntis Session
- Aufrufen eines manipulierten Links
- Sowohl WebUntis als auch die manipulierte Seite mussten im selben Browser aufgerufen werden

Cross-Site-Scripting
Wenn ein Angreifer im Besitz eines gültigen WebUntis Zugangs war (Benutzername + Passwort) war es möglich, JavaScript Code einzuschleusen und damit diverse Informationen auszulesen oder zu manipulieren – allerdings ausschließlich im Rahmen der Berechtigungen des betreffenden Benutzers.

Wir möchten uns bei allen Stellen bedanken, die uns auf diese Punkte aufmerksam gemacht haben. Auf die Schließung dieser Schwachstellen hatten wir bereits in den Release Notes hingewiesen, nachdem es aber nun Nachfragen zu diesem Thema gab, möchten wir Sie nun auch über diesen Weg noch einmal darüber in Kenntnis setzen.

Sind meine Daten sicher?
Ja. Wir haben nach Bekanntwerden der Lücken sofort technische und organisatorische Maßnahmen ergriffen, um die Ausnützung dieser zu unterbinden. In unseren Logs kann diesbezüglich kein Nachweis gefunden werden, die auf eine Ausnützung der benannten Lücken hindeutet. Das bedeutet, dass wir mit sehr hoher Wahrscheinlichkeit ausschließen können, dass Daten manipuliert oder unrechtmäßig eingesehen wurden.

Muss ich als WebUntis Administrator jedwede Schritte unternehmen?
Gemäß Artikel 33 EU-DSGVO gilt: “Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.”
Nachdem wir mit sehr hoher Wahrscheinlichkeit ausschließen können, dass Daten manipuliert oder unrechtmäßig eingesehen wurden, sind aus unserer Sicht für Sie keine weiteren Schritt zu unternehmen.

Ihr WebUntis Team

UID-Nr.: ATU69811938
Bankverbindungen:
Österreich - UniCredit Bank Austria AG
KtoNr.: 50800527000
IBAN: AT84 1200 0508 0052 7000
BIC: BKAUATWW
Deutschland - DZ Bank AG
IBAN: DE19 7016 0000 0000 1238 37
BIC: GENODEFF701