

Sicherheitshinweis: ProCall Enterprise Anfälligkeit für Remote-Code-Execution (http)

Knowledgebase

Exported on 01/12/2021

Table of Contents

1 Beschreibung	4
2 Betroffene Versionen	5
3 Workaround.....	6
4 Versionen mit Behebung des Problems.....	7

Veröffentlichungsdatum	 12.01.2021
Referenz	SIX-2492
Kritikalität	CRITICAL
CVSS-Score	9.4 ¹

¹ <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:X/RC:X&version=3.1>

1 Beschreibung

Eine Schwachstelle der Chat-Implementierung des ProCall Client für Windows könnte es Angreifern mit Zugriff auf die Chat-Funktionalität von ProCall Enterprise über das Netzwerk erlauben, Befehle durch eine Chat-Nachricht auszuführen.

Die Schwachstelle beruht auf unzureichender Behandlung von Links im Chat-Fenster des ProCall Client für Windows. Dadurch wäre es einem Angreifer theoretisch möglich, im zugrundeliegenden Microsoft Internet Explorer über das Netzwerk, d.h. von einem anderen ProCall Client, über das Kontaktportal oder die Multimedia Visitenkarte oder Federation, Befehle (z. B. JavaScript, ActiveX) auszuführen. Um die Schwachstelle auszunutzen, benötigt der Angreifer Zugriff auf die Chat-Funktionalität von ProCall Enterprise.

estos hat bereits ein Softwareupdate veröffentlicht, um die Schwachstelle zu adressieren. Als Workaround kann die Chat-Funktionalität von ProCall Enterprise vorübergehend deaktiviert werden.

2 Betroffene Versionen

Diese Schwachstelle betrifft alle bisher veröffentlichten Versionen von ProCall 6 Enterprise und ProCall 7 Enterprise.

- 7.0, 7.1 (alle Unterversionen)
- 6.0, 6.1, 6.2, 6.3, 6.4 (alle Unterversionen)

3 Workaround

Als Workaround kann die Chat-Funktionalität [vollständig deaktiviert](#)² werden, um den Aufruf des Chat-Fensters zu verhindern.

² https://help.estos.com/help/de-DE/procall/7/ucserver/dokumentation/tapisrv/IDD_BASESERVICES.htm

4 Versionen mit Behebung des Problems

estos hat bereits Updates mit Behebungen der Schwachstelle veröffentlicht. Kunden und Partner können die Updates über die bekannten Kanäle beziehen und dem normalen Update-Prozess folgen.

- ProCall 7 Enterprise \geq 7.1.2.3786
- ProCall 6 Enterprise \geq 6.4.15.3785