Security advisory: ProCall Enterprise remote code execution vulnerability (http)

Knowledgebase

Exported on 01/12/2021

Table of Contents

Release date	12.01.2021
Reference	SIX-2492
Criticality	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 Description

A vulnerability in the chat implementation of ProCall client for Windows could allow hackers with access to the chat functionality of ProCall Enterprise over the network to execute commands through a chat message.

The vulnerability is due to inadequate handling of links in the chat window of the ProCall client for Windows. This would theoretically allow a hacker to execute commands (e.g. JavaScript, ActiveX) in the underlying Microsoft Internet Explorer over the network, i.e. from another ProCall client, via the contact portal or the multimedia business card or federation. To exploit the vulnerability, the hacker needs access to the chat functionality of ProCall Enterprise.

estos has already released a software update to address the vulnerability. As a workaround, the chat functionality of ProCall Enterprise can be temporarily disabled.

2 Affected versions

This vulnerability affects all previously released versions of ProCall 6 Enterprise and ProCall 7 Enterprise.

- 7.0, 7.1 (all sub-versions)
- 6.0, 6.1, 6.2, 6.3, 6.4 (all sub-versions)

3 Workaround

As a workaround, the chat functionality can be completely disabled[2] to prevent the chat window from opening.

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

4 Versions with bug fixes

estos has already released updates with fixes to the vulnerability. Customers and partners can obtain updates through the known channels and follow the normal update process.

- ProCall 7 Enterprise ≥ 7.1.2.3786
- ProCall 6 Enterprise ≥ 6.4.15.3785