Security Incident Management

Incident reported by:	*Date:*
Media	03.07.2020

Referenced Documents:
none

Incidents covered by this document:
• Vulnerability SIM#2020-03-a: "out-of-bounds error in rdpsnd" • Vulnerability SIM#2020-03-b: "memory safety violation in guac_common_svc.c"

VDE-ID:
VDE-2021-031

Public disclosure:	*Date:*
Incident-Report - SIM#2020-03	22.07.2021
mbCONNECT24/mymbCONNECT24 - Firmware 2.9.0	27.05.2021

The MB connect line security team can be reached via email at security-team@mbconnectline.com. For incident-reports, please use encypted communication only. For details and PGP-credentials visit https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

More information on current threats and the associated product safety of our devices and software solutions can be found at https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

All vulnerability-metrics used in this document are created with the NIST NVD CVSS-Calculator V3 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Document: SIM#2020-03 / Rev.: 5
Created by:fade / 2021-07-22

Vulnerability SIM#2020-03-a:
"out-of-bounds error in rdpsnd"

Details

CVE: CVE-2020-9497
Description: Apache Guacamole 1.1.0 and older do not properly validate data received from RDP servers via static virtual channels. If a user connects to a malicious or compromised RDP server, specially-crafted PDUs could result in disclosure of information within the memory of the guacd process handling the connection.
Solution: Update to 2.9.0.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.8.0	2.9.0

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-200
CVSS Base Score:	4.4
CVSS v3 Link:	AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N

MB connect line GmbH
Winnettener Str. 6
D-91550 Dinkelsbühl

+49 (0) 9851 / 58 25 29 0
+49 (0) 9851 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2020-03-b:
"memory safety violation in guac_common_svc.c"

Details

CVE: CVE-2020-9498
Description: Apache Guacamole 1.1.0 and older may mishandle pointers involved in processing data received via RDP static virtual channels. If a user connects to a malicious or compromised RDP server, a series of specially-crafted PDUs could result in memory corruption, possibly allowing arbitrary code to be executed with the privileges of the running guacd process.
Solution: Update to 2.9.0.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.8.0	2.9.0

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-119
CVSS Base Score:	6.7
CVSS v3 Link:	AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Document: SIM#2020-03 / Rev.: 5
Created by:fade / 2021-07-22

MB connect line GmbH
Winnettener Str. 6
D-91550 Dinkelsbühl

+49 (0) 9851 / 58 25 29 0
+49 (0) 9851 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com