PSIRT Advisories

ID STW-IR-23-001

Published 16.05.2023 13:28 (CEST)

Last update 18.07.2023 15:35 (CEST) – Updated Summary

Severity Critical

CVSSv3 Score 10

Product(s)

Article Number	Product Name	Affected Version(s)
86841, 86842, 86843, 86844, 86878, 86912, 86913, 88267, 88268, 88269, 88270, 90262, 91200, 91201, 92268, 92269, 92325, 92443, 92444, 92445, 92537, 92648, 93493, 93494, 93495, 93629, 94091, 94138, 94139, 100301, 100440, 100888, 103260, 104108, 105045, 105046, 107685	TCG-4	DeploymentPackage_v3.03r0-Impala DeploymentPackage_v3.04r2-Jellyfish Out of Support, but still affected: DeploymentPackage_v3.01r1-Gecko DeploymentPackage_v3.02r0-Hedgehog
107143, 105772, 103489	TCG-4lite	DeploymentPackage_v3.04r2-Jellyfish

Summary

The execution of stw_RecvSMS utility or using SMS wakeup option in STW TCG-4 Automotive Connectivity Module and TCG-4lite Automotive Connectivity Module (no SMS wakeup implemented) allows Eval Injection.
This allows an attacker to gain full remote access with Root privileges without the need for authentication, giving an attacker arbitrary remote code execution over LTE / 4G network via crafted payload injected into SMS. Moreover, under special circumstances the vulnerability can wake up the device to execute arbitrary remote code even when the ignition is off.

The bug fixes were made available via the customer download area on 16.05.2023 13:28 (CEST).

CVE ID CVE-2023-35830

Impact Eval Injection, CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code.

Affected Components

- stw_RecvSMS (< obs_v1_04r3)
- SMS_WAKEUP=ON as boot option

Solution Please upgrade to DeploymentPackage_v3_06r0-Koala or use the Bugfix for corresponding Deployment Package:

- DeploymentPackage_v3.03r0-Impala-BUG1
- DeploymentPackage_v3.04r2-Jellyfish-BUG3

Reported by The vulnerability was reported by Abdallah Mola and Maria Blumenröhr from EDAG Engineering GmbH on 02.05.2023 13:00 (CEST).

Adresse
Am Bärenwald 6
87600 Kaufbeuren
Deutschland
Internet
www.stw-mm.com

Telefon
+49 8341 9505-0
Fax
+49 8341 9505-55
E-Mail
info.stw@wiedemann-group.com

Sitz der Gesellschaft
Kaufbeuren
Registergericht
Kempten HRB 1863

Geschäftsführung
Christophe de Bary
Steffen Dieterle
Sonja Wiedemann

USt. ID-Nr.
DE 811 355 522
St.-Nr.
125/137/30002

Bankverbindung
Baden-Württembergische Bank
IBAN DE86 6005 0101 0001 0009 06
BIC SOLADEST600

Bankverbindung
Sparkasse Kaufbeuren
IBAN DE75 7345 0000 0000 0219 72
BIC BYLADEM1KFB