

PSIRT Advisories

ID STW-IR-23-001
Published 16.05.2023 13:28 (CEST)
Last update 22.06.2023 15:35 (CEST)
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
	107143, 105772, 103489	TCG-4lite	DeploymentPackage_v3.04r2-Jellyfish

Summary This vulnerability allows an attacker to gain full remote access with Root privileges without the need for authentication, it gives an attacker arbitrary remote code execution over LTE / 4G network via SMS.

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

CVE ID [CVE-2023-35830](#)

Impact Authentication bypass

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).