CTOne
Vulnerability Disclosure Policy

Goal

This program aims to assist researchers and vendors in the responsible disclosure of vulnerabilities reported to CTOne.

CTOne handles responsible vulnerability disclosure to product vendors, CTOne customers, security vendors, and the general public. CTOne will responsibly and promptly notify the appropriate product vendor of a security flaw with their product(s) or service(s).

About TR2

Our TR2 (Threat Research and Response) team is a dedicated threat & attack intelligence team, delivering in-depth cybersecurity knowledge and threat expertise, which helps enterprises improve the overall security posture of a private wireless deployment.

TR2 specializes in private cellular networks; covering threats and attacks in packet-core, RAN and cellular IoT devices.
Together with Trend Micro for IT threat intelligence, we conduct forward-looking threat research, perform security testing, and develop mitigations for emerging and future attacks.

Procedure

Once a vulnerability report is received, we will acknowledge the receipt of the report in 2 business days. The report will be reviewed to see if it falls under the scope of our program. The reporter will be notified in 3 business days. (The reporter may be requested for further clarifications if necessary. Thereafter, CTOne will attempt to contact the affected vendor.)

Action after receiving your submission

CTOne will attempt to contact the vendor through the Product Security Incident Response Team (PSIRT) mechanisms listed on their website. If PSIRT information is not available, other contact options available on the website will be tried. If the vendor responds within 15 days, a 90-day Withholding Period will be allowed for the vendor to fix the issue and release patches. In exceptional circumstances, the period may be extended, up to a maximum of 180 days in total.After the end of the withholding period, a public advisory will be released on the CTOne website.

Past the 5-Day Deadline

If there is no acknowledgment of receipt from the vendor after 5 days, a second attempt will be made to contact a representative.

Past the 15-Day Deadline

If there is no acknowledgment of receipt from the vendor after 15 days of the initial contact attempt, a public advisory will be released on the CTOne website.

Reward

If the vendor offers rewards for the report, all efforts will be made to avail it to the vulnerability reporter.

Our Scope

Vulnerabilities in Cellular (LTE/4G/5G) devices and protocols.

What is covered?

- Any Vulnerability in Cellular infrastructure devices such as packet-core (EPC, 5GC),
- RAN nodes (gNB, eNB, ORAN).
- Any Vulnerability in Cellular IoT devices (CIoT); CIoT devices are IoT devices with a
- cellular interface. E.g.: sensors, routers, cameras, drones…etc.
- Protocol Vulnerabilities in Cellular Technology (CT) protocols such as GTP, NGAP, PFCP, E2AP, F1AP on any device.

What is not covered?

- Radio protocol level vulnerabilities (RRC).
- Application Vulnerabilities on Smart-Phones.

CTOne contact information

Email us at: tr2@ctone.com.

CTOne, a global cybersecurity leader in communication technology/ a subsidiary of Trend Micro, with over 30 years of experience in information technology (IT) security inherited from Trend Micro, CTOne bridges the communication technology (CT) gap by dedicating resources to the development of enterprise cybersecurity. On top of providing the most comprehensive solution in terms of mobile network communication protection, CTOne helps enterprises integrate IT and CT technologies for digital transformation, reducing operating costs, increasing productivity, and avoiding significant losses. CTOne is constantly on guard to ensure that daily business operations are protected to keep enterprises at the forefront of the market.

www.ctone.com