T82 THE CLAROTY RESEARCH TEAM

CLAROTY

EXECUTIVE SUMMARY: 1H 2022

STATE OF XIOT SECURITY

Team82's analysis of vulnerabilities impacting cyber-physical systems across the Extended Internet of Things

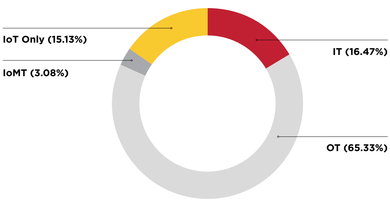
XIoT Vulnerabilities Breakdown

Team82 has revamped its biannual report to embrace an understanding of the vulnerabilities being disclosed and fixed within the Extended Internet of Things (XIoT). XIoT is the umbrella term for connected cyber-physical devices within industrial, healthcare, and commercial enterprise IoT environments.

This report is a reflection of the need to secure the cyber-physical systems that enable our ability to innovate and sustain our lives. We hope the State of XIoT Security report is a useful resource for you.

While published operational technology vulnerabilities dominate Team82's dataset for the 1H 2022, it's important to note that IoT vulnerabilities have almost doubled since our last report, especially impacting connected smart devices, routers and other networking gear, and cameras—all of which if compromised may afford an attacker deeper access to the enterprise network.

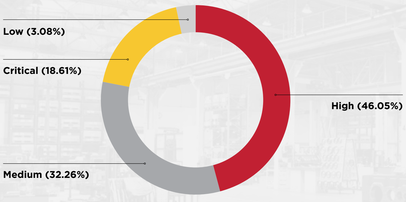
XIoT VULNERABILITIES BREAKDOWN



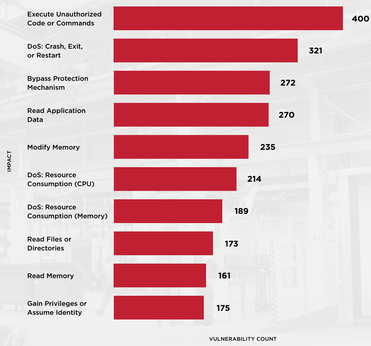
Criticality and Impact

The vast majority of published XIoT vulnerabilities in the 1H of 2022 were either critical or high severity.

Of those critical and high-severity vulnerabilities, many affect the availability of XIoT devices and enable code execution or denial of service attacks.



VULNERABILITY COUNT BY IMPACT TOP 10



Let's Talk About Firmware

Updating firmware presents challenges, yet with the rise in connected devices across industries, Team82's dataset shows a spike in published firmware vulnerabilities, and marked improvement in remediations. More companies understand the need to secure connected OT, IoT, and IoMT devices, and firmware fixes are a big step forward.

Below, you can see that for the 1H 2022, the number of published firmware vulnerabilities is almost on par with software vulnerabilities, a significant reversal from the 2H 2021 report when there was an almost 2-to-1 disparity between software and firmware vulnerabilities.

SOFTWARE

FIRMWARE

1H 2022

40%

Fully or partially remediated firmware vulnerabilities

2H 2021

21%

Fully or partially remediated firmware vulnerabilities

Key Events Timeline

April

Industroyer2: Industroyer variant uncovered in foiled attack against Ukrainian electricity provider

Incontroller (aka Pipedream): ICS attack platform purpose-built to target PLCs and critical infrastructure

May

Team82's 300 CVE to-date is published.

June

OT:ICEFALL: 56 vulnerabilities affecting devices from 10 XIoT vendors

Remediations and Mitigations

Team82's 1H 2022 dataset indicates that vendors provided full or partial remediation for 91% of published vulnerabilities.

REMEDIATION BY THE NUMBERS

71%

Full remediation: All products are patched and updated

20%

Partial remediation: Not all affected products have a fix

9%

No remediation: Product remains unpatched, and without mitigations

T82 THE CLAROTY RESEARCH TEAM

CLAROTY