



USE CASE

From Hours to Seconds

**Simplify Your Attack Path Analysis
With xZETA**



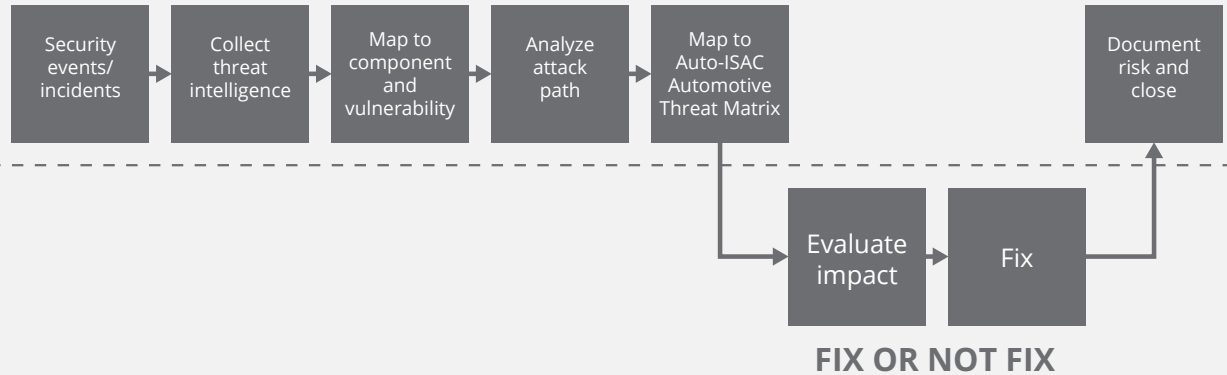
How xZETA Enables the PSIRT to Focus on Incident Response — the Most Critical Task

B
E
F
O
R
E

PSIRT



IDENTIFY AND ASSESS



OEM and suppliers
PSIRT/Product development team

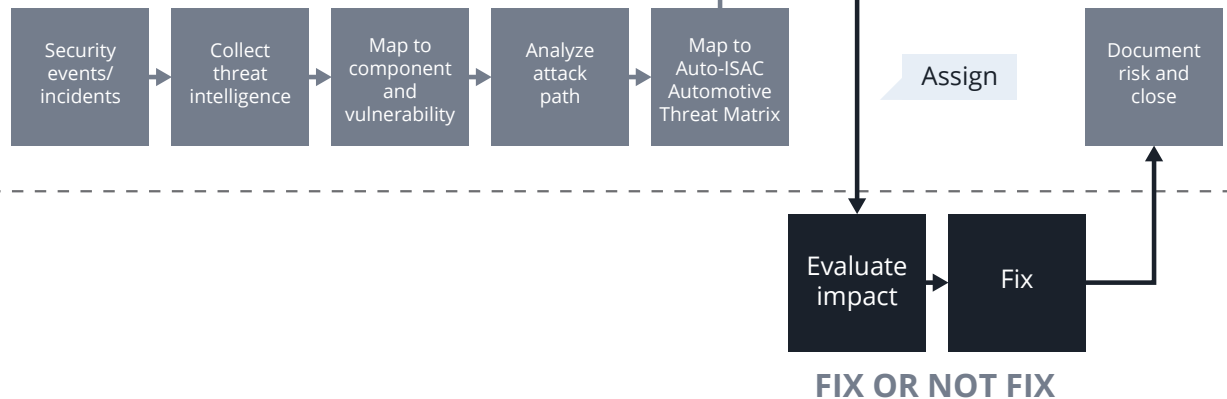
FIX OR NOT FIX

A
F
T
E
R

PSIRT



IDENTIFY AND ASSESS



OEM and suppliers
PSIRT/Product development team

FIX OR NOT FIX



USE CASE

Zero-Click Exploit Targeting MCUs: Taking Control of the IVI via Wi-Fi

██████'s Zero-click Vulnerabilities Allowed its Car to be Hacked Remotely Using Drones

The zero-click vulnerabilities, which the researchers named "TBONE," were originally scheduled to be showcased at ██████'s "Pwn2Own 2020" hacking event.

🚩 CVE-2021-3347 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.

Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: **7.8 HIGH**

Vector:

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A
F
T
E
R

PSIRT



OEM and suppliers

PSIRT / product development team

1

ISO/SAE 21434 8.3 "Cybersecurity monitoring"

IDENTIFY AND ASSESS



Qualify incident

Assign

Document risk and close

Evaluate impact

Fix

FIX OR NOT FIX

Incident details

Related vulnerabilities

Maps the incident's attack path with relevant exploited vulnerabilities

Summary

Attack type: ZDI
Approach: Short-Range Wireless Communication
Affected vendor:
Target: Wi-Fi, IVI System
Impact: Vehicle

Description

Researchers Ralf-Philipp and Benedikt Schmotzle discovered a remote zero-click security vulnerability in an open-source component in automobiles. Hackers who use this vulnerability can gain control over the car's infotainment system remotely over Wi-Fi. Thankfully, this attack will not allow hackers drive control.

2024-06-11 | Source

Attack Phase Overview

Manipulate Environment

Persistence

Lateral Movement

Affect Vehicle Function

Impact

Attack path with TTPs

Activity	Technique ID
1 Initial entry over Wi-Fi.	T1465 - Rogue Wi-Fi Access Points
2 Exploit DHCP stack.	T1210 - Exploitation of Remote Services
3 Privilege escalation on the MCU.	T1404 - Exploitation for Privilege Escalation

View UN R155 Reference

Attack phase

Manipulate Environment

Lateral Movement

Persistence

Persistence

A
F
T
E
R

PSIRT



OEM and suppliers
PSIRT / product development team

IDENTIFY AND ASSESS



2

Qualify incident

Assign

Document risk and close

Evaluate impact

Fix

ISO/SAE 21434
8.4 "Cybersecurity event evaluation"
8.5 "Vulnerability analysis"

FIX OR NOT FIX

Incident: Zero-Click Exploit for MCUs

Incident details Related vulnerabilities

Recommendation
Update to the latest firmware which has already

Affected firmware

Vulnerability: CVE-2021-3347

Original CVSS rating: 7.8 High

Company or model

Affected firmware	VVIR ⓘ ↓	Phase	Processor	Operating system	Firmware profile	Detection time
MCU-2021-12	4.5 Medium	Development	ARM 64-bit	Linux 64-bit	Provider: - Destination: -	2024-02-16 18:00:17
MCU-2021-11	4.5 Medium	Development	ARM 32-bit	Android 32-bit	Provider: - Destination: -	2023-01-04 11:36:24
MCU-2021-10	4.5 Medium	Release	ARM 64-bit	Linux 64-bit	Provider: - Destination: -	2022-12-15 16:54:05
MCU-2021-09	4.5 Medium	Development	ARM 64-bit	Linux 64-bit	Provider: - Destination: -	2023-05-18 14:50:28
MCU-2021-08	4.5 Medium	Development	ARM 32-bit	Linux 32-bit	Provider: SUP3 Destination: OEM3 MD333	2025-01-10 16:13:46
MCU-2021-07	4.5 Medium	Development	ARM 32-bit	Linux 32-bit	Provider: - Destination: -	2022-12-15 16:54:05

Total: 18 25 per page 1 / 1

Detection time: 2024-07-23

Affected firmware Published

17 2021-01-30

Total: 1 25 per page 1 / 1

With this information, the PSIRT can assess and qualify the incident. xZETA also provides details on:

- affected firmware versions
- involved devices
- responsible department or supplier
- impacted customers

A
F
T
E
R

PSIRT



OEM and suppliers

PSIRT / product development team

IDENTIFY AND ASSESS

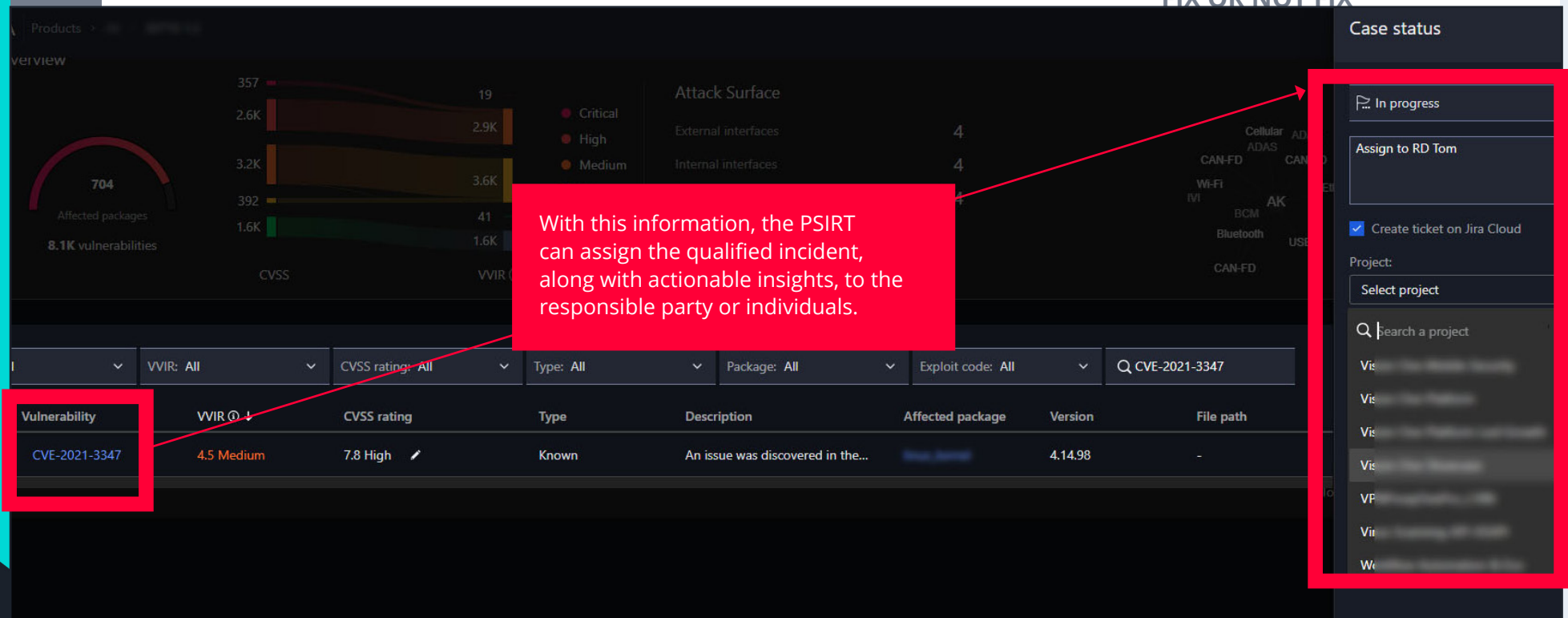


ISO/SAE 21434

8.4 "Cybersecurity event evaluation"

8.5 "Vulnerability analysis"

FIX OR NOT FIX



A
F
T
E
R

PSIRT



OEM and suppliers

PSIRT / product development team

IDENTIFY AND ASSESS



Qualify incident

Assign

Evaluate impact

Fix

Document risk and close

FIX OR NOT FIX

**ISO/SAE 21434
8.6 "Vulnerability management"**

4

Status: All	VVIR: All	CVSS rating: All	Type: All	Package: All	Exploit code: All	Q Vulnerability ID or ke			
☐	Vulnerability	VVIR	CVSS rating	Type	Description	Affected package	Version	File path	Expl code
☐	CVE-2014-6271	9.8 Critical	9.8 Critical	Known	GNU Bash through 4.3 process...	bash	4.2.46	/usr/bin/bash	✓
☒	Closed CVE-2021-3347	Once the incident is resolved, a note is added to the system to close the case.				linux_kernel	4.14.98	-	-
☐	CVE-2018-5740	7.9 High	7.5 High	Known	"deny-answer-aliases" is a littl...	bind- license	9.11.4	/usr/share/licenses/bind-licens...	-
☐	CVE-2020-8617	7.5 High	5.9 Medium	Known	Using a specially-crafted mess...	bind- license	9.11.4	/usr/share/licenses/bind-licens...	✓
☐	CVE-2020-8625	7.2 High	8.1 High	Known	BIND servers are vulnerable if ...	bind- license	9.11.4	/usr/share/licenses/bind-licens...	-
☐	CVE-2021-25216	6.7 Medium	9.8 Critical	Known	In BIND 9.5.0 -> 9.11.29, 9.12....	bind- license	9.11.4	/usr/share/licenses/bind-licens...	-

xZETA

Superior Automotive Vulnerability and SBOM Management System

Gather



Binaries/
Firmware



Third-party
SBOM

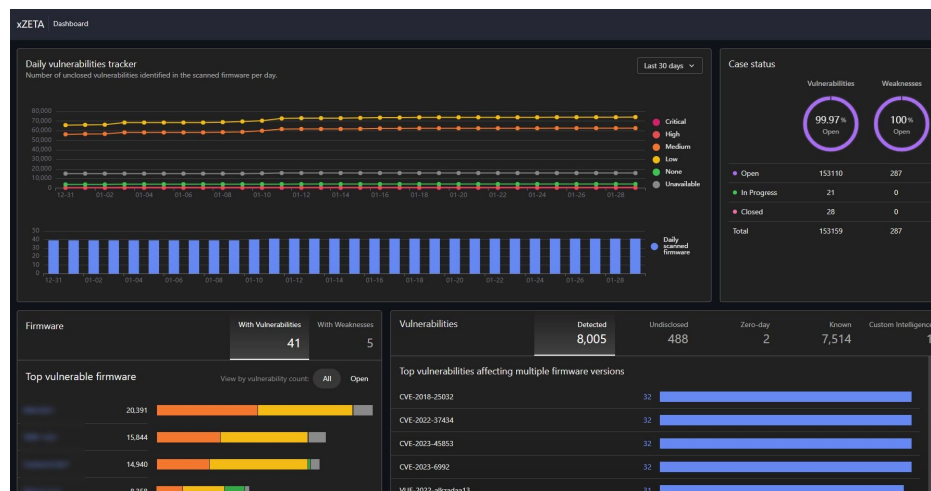


Third-party
HBOM



Open-source/
Third-party
application

xZETA



Achieve With Ease

XBOM management

Vulnerability management

APT/Ransomware detection

Private vulnerability
database creation

Sensitive data leak detection

License compliance



Gain Instant Access to Automotive Threat Intelligence

xZETA offers automotive threat intelligence, tracking global cybersecurity incidents and correlating them with vulnerabilities. This helps OEMs and suppliers understand exploitation methods and **map attack paths with context**.



Get the Best Coverage With 189% More

xZETA provides 189% more coverage than the National Vulnerability Database (NVD), including **zero-day vulnerabilities, undisclosed risks, customer-discovered vulnerabilities**, and more.



Enhance Operational Efficiency

xZETA streamlines the ISO/SAE 21434 workflow with seamless **TARA tool integration** and smooth connectivity to **third-party ticketing systems** for efficient case management.



Reduce Attack Path Analysis Time From Hours to Seconds

Enabling Faster Response and Mitigation With xZETA

REQUEST A DEMO

xZETA
Copyright © 2025 VicOne Inc.
All Rights Reserved.

Learn more about VicOne
by visiting VicOne.com or
scanning this QR code:

