VicOne

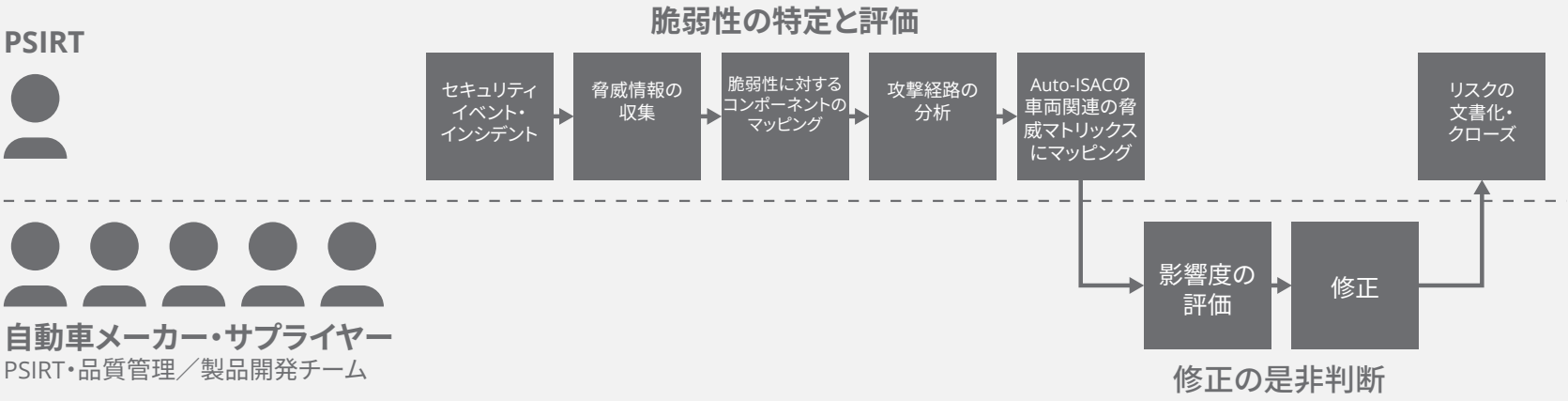
導入事例

時間から秒へ

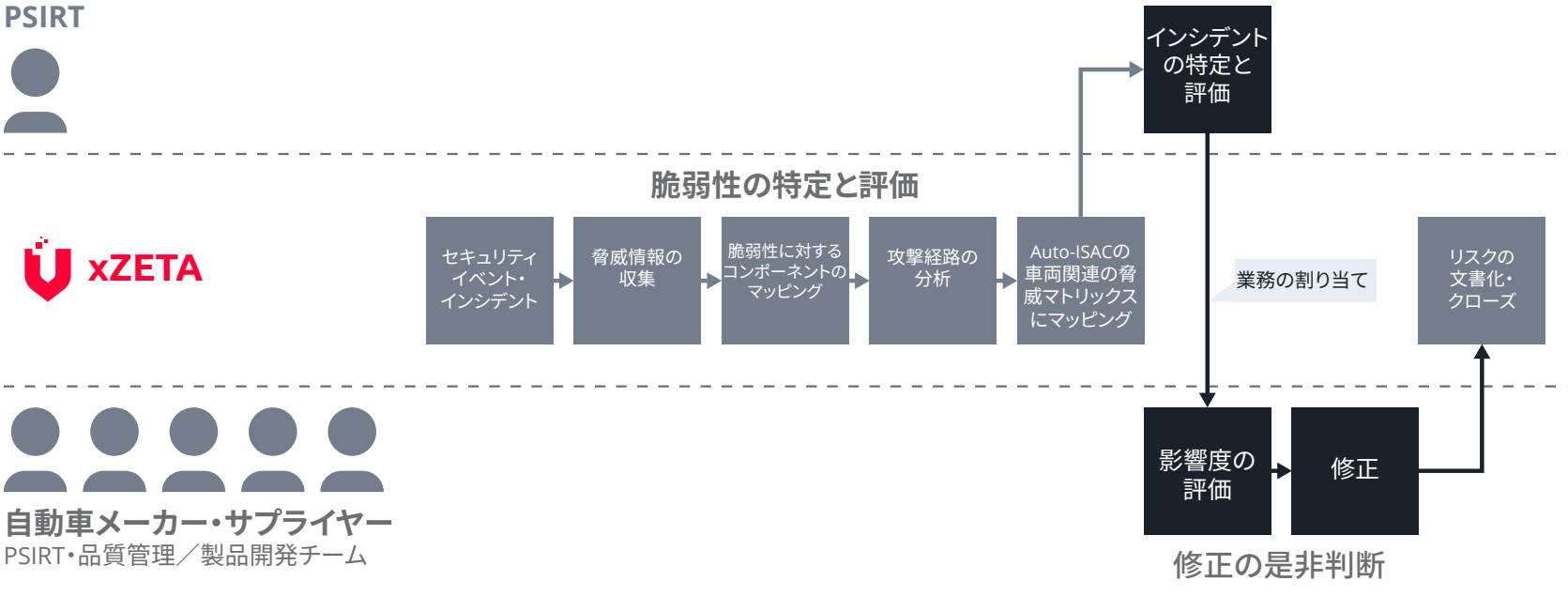
xZETAで攻撃経路分析を迅速化

xZETAは煩雑な手作業を自動化―PSIRTチームは最優先タスクであるインシデントレスポンスに集中可能に

導入前



導入後



導入事例

MCUを標的としたゼロクリック攻撃：Wi-Fi経由でIVIを制御

[redacted]のゼロクリックの脆弱性により、ドローンを使用して車が遠隔操作でハッキングされる可能性

研究者が「TBONE」と名付けたゼロクリックの脆弱性は、当初、[redacted]のハッキングイベント「Pwn2Own 2020」で展示される予定でした。

CVE-2021-3347 詳細

修正済み

このCVEレコードは、NVDエンリッチメント作業が完了した後に更新されました。NVDによって提供されるエンリッチメントデータは、これらの変更により修正が必要になる場合があります。

説明

Linuxカーネル5.10.11で問題が発見されました。PI futexには、障害処理中にカーネルスタックの解放後使用があり、ローカルユーザーがカーネル内でコードを実行できる可能性があります(CID-34b1a1ce1458)。

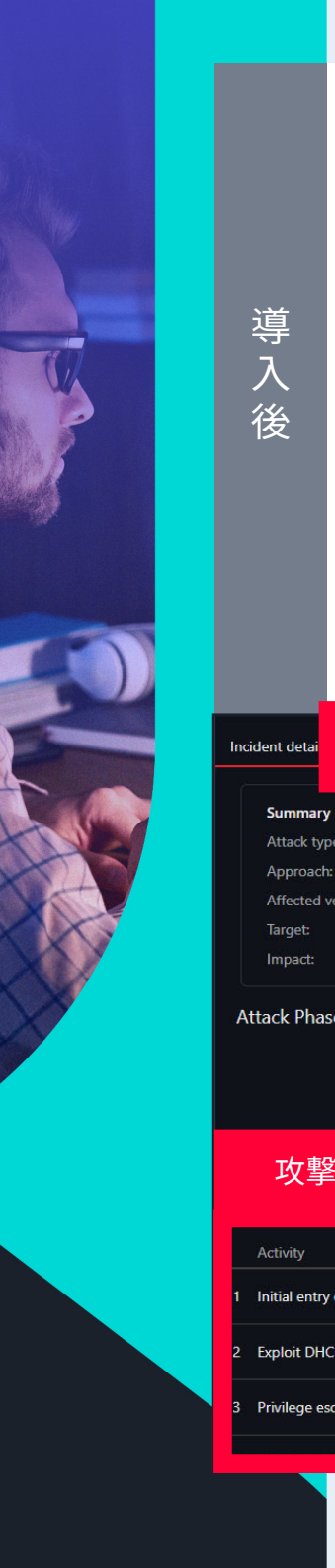
メトリクス

CVSSバージョン4.0 | CVSSバージョン3.x | CVSSバージョン2.0

NVDエンリッチメントの取り組みでは、ベクター文字列を関連付けるために公開されている情報を参照します。他のソースから提供されたCVSS情報も表示されます。

CVSS 3.xの重大度とベクトル文字列:

NIST: NVD　**基本スコア:** 7.8 高　**ベクトル:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



導入後

PSIRT

xZETA

1 ISO/SAE 21434 8.3「サイバーセキュリティ監視」

脆弱性の特定と評価

セキュリティイベント・インシデント → 脅威情報の収集 → 脆弱性に対するコンポーネントのマッピング → 攻撃経路の分析 → Auto-ISACの車両関連の脅威マトリックスにマッピング

インシデントの特定と評価

業務の割り当て

リスクの文書化・クローズ

影響度の評価 → 修正

修正の是非判断

自動車メーカー・サプライヤー

PSIRT・品質管理／製品開発チーム

インシデントの攻撃経路と関連する悪用された脆弱性をマッピング

Incident detai | Related vulnerabilities

Summary

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

- In vehicle (1): IVI System

Description 2024-06-11 Source

Researchers Ralf-Philipp and Benedikt Schmotzle discovered a remote zero-click security vulnerability in an open-source component in [redacted] 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.

Attack Phase Overview

Manipulate Environment → Persistence → Lateral Movement → Affect Vehicle Function → Impact

攻撃経路とTTP（サイバー攻撃における戦術、技術、手法の特性）

View UN R155 Reference

	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

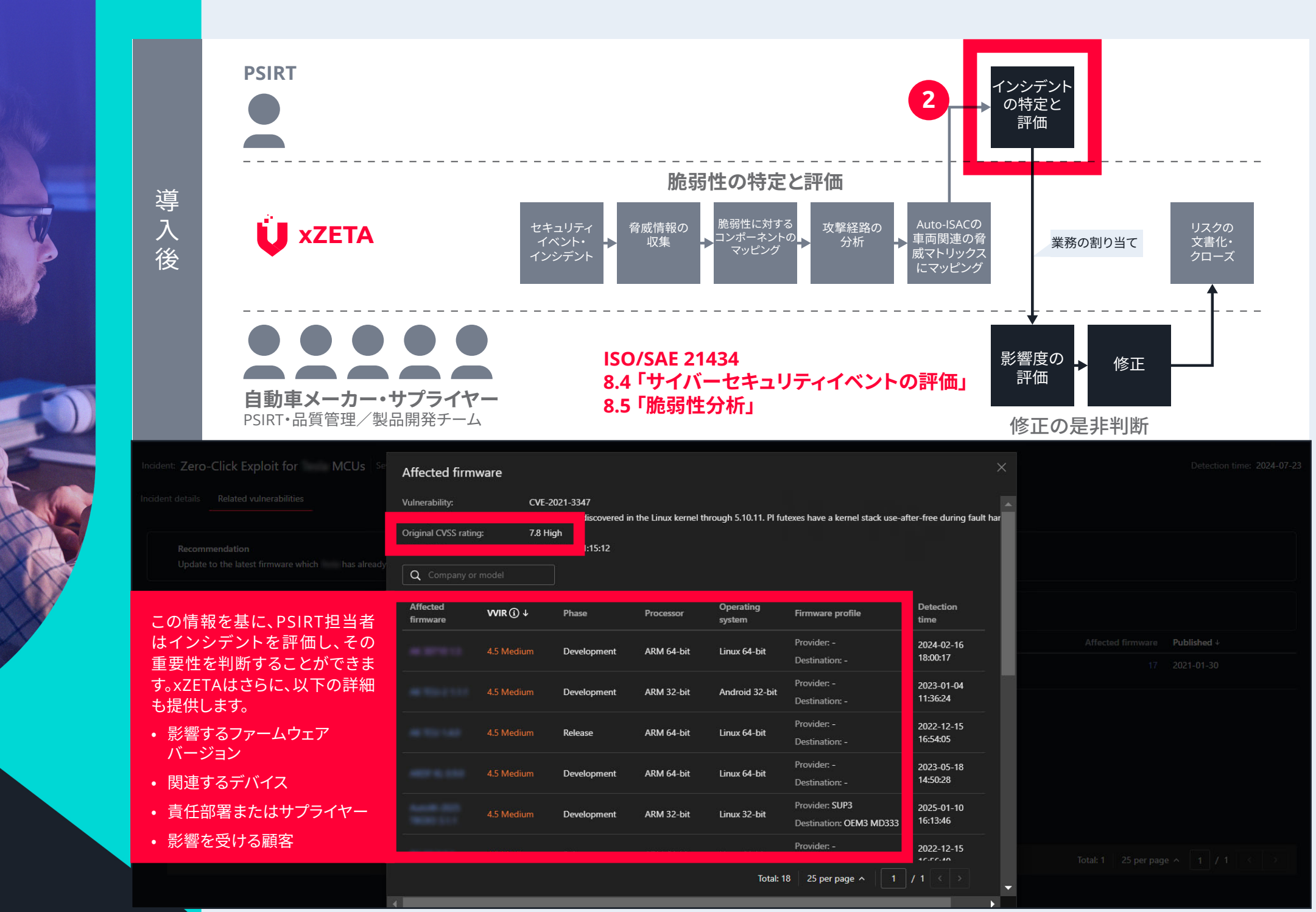
Attack phase

Manipulate Environment

Lateral Movement

Persistence

Persistence


導入後
PSIRT
xZETA
2
インシデントの特定と評価
脆弱性の特定と評価
セキュリティイベント・インシデント
脅威情報の収集
脆弱性に対するコンポーネントのマッピング
攻撃経路の分析
Auto-ISACの車両関連の脅威マトリックスにマッピング
業務の割り当て
リスクの文書化・クローズ
自動車メーカー・サプライヤー
PSIRT・品質管理／製品開発チーム
ISO/SAE 21434
8.4「サイバーセキュリティイベントの評価」
8.5「脆弱性分析」
影響度の評価
修正
修正の是非判断
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
4.5 Medium
Development
ARM 64-bit
Linux 64-bit
Provider: -
Destination: -
2024-02-16 18:00:17
4.5 Medium
Development
ARM 32-bit
Android 32-bit
Provider: -
Destination: -
2023-01-04 11:36:24
4.5 Medium
Release
ARM 64-bit
Linux 64-bit
Provider: -
Destination: -
2022-12-15 16:54:05
4.5 Medium
Development
ARM 64-bit
Linux 64-bit
Provider: -
Destination: -
2023-05-18 14:50:28
4.5 Medium
Development
ARM 32-bit
Linux 32-bit
Provider: SUP3
Destination: OEM3 MD333
2025-01-10 16:13:46
Provider: -
2022-12-15
Total: 18
25 per page
1 / 1
この情報を基に、PSIRT担当者はインシデントを評価し、その重要性を判断することができます。xZETAはさらに、以下の詳細も提供します。
• 影響するファームウェアバージョン
• 関連するデバイス
• 責任部署またはサプライヤー
• 影響を受ける顧客

導入後

PSIRT

xZETA

脆弱性の特定と評価

セキュリティイベント・インシデント → 脅威情報の収集 → 脆弱性に対するコンポーネントのマッピング → 攻撃経路の分析 → Auto-ISACの車両関連の脅威マトリックスにマッピング → インシデントの特定と評価 → 業務の割り当て → リスクの文書化・クローズ

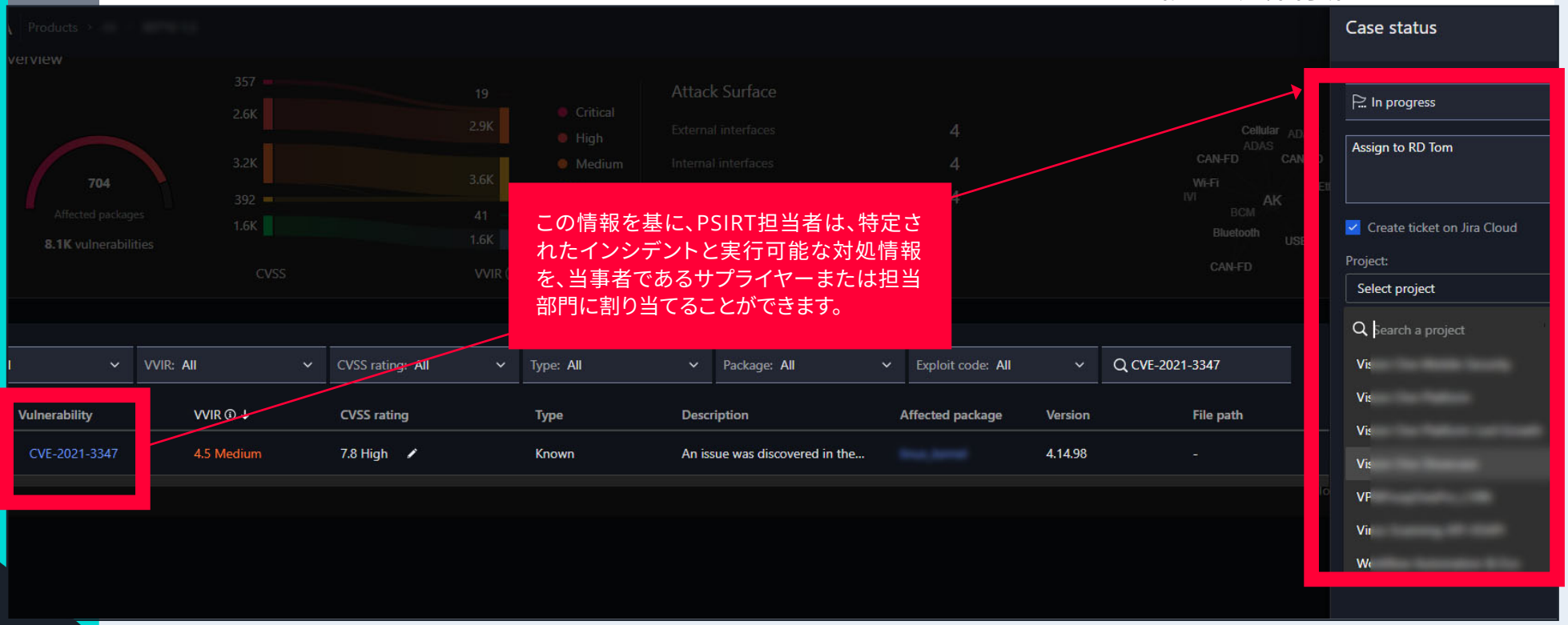
3

自動車メーカー・サプライヤー
PSIRT・品質管理／製品開発チーム

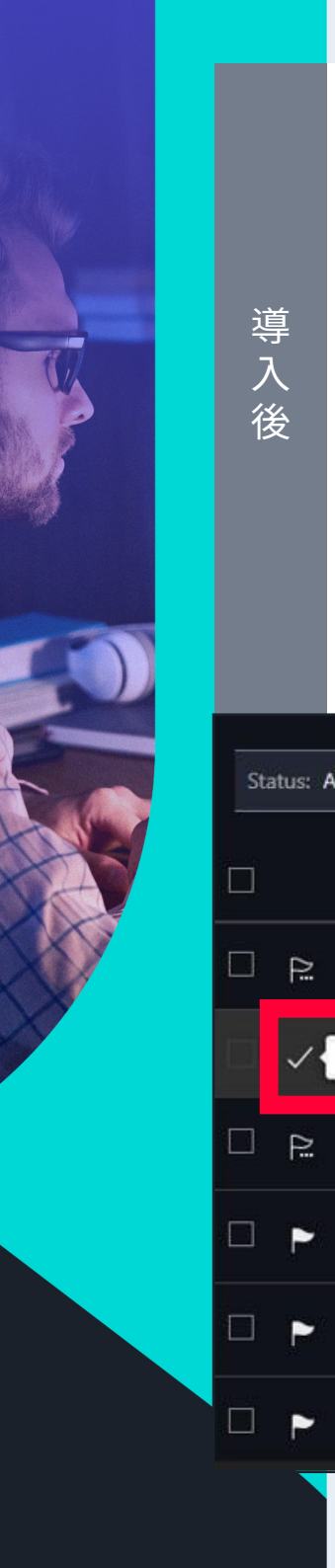
ISO/SAE 21434
8.4「サイバーセキュリティイベントの評価」
8.5「脆弱性分析」

影響度の評価 → 修正

修正の是非判断



この情報を基に、PSIRT担当者は、特定されたインシデントと実行可能な対処情報を、当事者であるサプライヤーまたは担当部門に割り当てることができます。



導入後

PSIRT

xZETA

ISO/SAE 21434
8.6「脆弱性管理」

脆弱性の特定と評価

セキュリティイベント・インシデント → 脅威情報の収集 → 脆弱性に対するコンポーネントのマッピング → 攻撃経路の分析 → Auto-ISACの車両関連の脅威マトリックスにマッピング → インシデントの特定と評価

業務の割り当て

4 リスクの文書化・クローズ

影響度の評価 → 修正

修正の是非判断

自動車メーカー・サプライヤー
PSIRT・品質管理／製品開発チーム

Status: All | VVIR: All | CVSS rating: All | Type: All | Package: All | Exploit code: All | Vulnerability ID or ke

	Vulnerability	VVIR	CVSS rating	Type	Description	Affected package	Version	File path	Expl cod
☐	CVE-2014-6271	9.8 Critical	9.8 Critical	Known	GNU Bash through 4.3 process...	bash	4.2.46	/usr/bin/bash	✓
✓	クローズ 021-3347				issue was discovered in the...	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...	-

問題が解決すると、システムにケースをクローズした事を示すメモが追加されます。

xZETA

自動車特化の卓越した脆弱性・SBOM管理システム

収集

- バイナリ／ファームウェア
- サードパーティのSBOM
- サードパーティのHBOM
- オープンソース／サードパーティアプリケーション

容易に達成

- XBOM管理
- 脆弱性管理
- APT／ランサムウェア検出
- 自社独自の脆弱性データベースの作成
- 機密データ漏洩検出
- ライセンス・コンプライアンスの確認

自動車関連の脅威インテリジェンスに即座にアクセス

xZETAは、世界的なサイバーセキュリティインシデントを追跡し、脆弱性との相関関係を分析した自動車業界向けの脅威情報を提供しています。これにより、OEMやサプライヤーは悪用手法を理解し、**コンテクストを伴う攻撃経路をマッピング**することができます。

189%増しの検出範囲で死角を排除

xZETAは、**ゼロデイ脆弱性、未公開のリスク、ユーザーが発見した脆弱性など**を含め、NIST(アメリカ国立標準技術研究所）が運営するセキュリティ脆弱性に関するデータベース（NVD: National Vulnerability Database）よりも189%多い情報を提供しています。

業務効率の向上

xZETAは、Jiraなどの**サードパーティのチケットシステム**やBlock Harborなどの**TARAツールとの連携**が可能。ISO/SAE 21434のワークフローを効率化し、効率的なケース管理を実現します。

VicOne

攻撃経路分析を数時間から数秒に短縮

xZETAで迅速な対応と危機回避を実現

お問い合わせ

詳しくはVicOneウェブサイトをご覧ください。
(VicOne.com/jpもしくは右記QRコードをスキャンしてアクセス)