Carnegie Mellon University
Software Engineering Institute

CERT Coordination Center Comments on NHTSA-2020-0087

Background

The CERT Coordination Center (CERT/CC) is part of the Software Engineering Institute (SEI) at Carnegie Mellon University. One focus area of the CERT/CC is the analysis, coordination, disclosure, and remediation of software vulnerabilities. This work dates back to the origin of the CERT/CC in 1988[1] and our comments are based on both practical experience and experimental research. The SEI is a DoD-sponsored FFRDC.

For questions about these comments please contact Laurie Tyzenhaus <latyzenhaus@cert.org>.

[1] http://www.mycal.net/Group42/hack/unix/cert/ca-88.01

Summary

Software vulnerabilities, security defects, security bugs, insecure configurations, insecurity caused by the unexpected interactions of complex systems: These are inherent aspects of all software systems, including those integrated into motor vehicles and transportation systems. It is economically (and likely technically) infeasible to produce software systems that are free of vulnerabilities. It is therefore critical that the manufacturers and suppliers of motor vehicle and transportation software systems have the capability to reduce and manage the risk posed by software vulnerabilities.[2]

We consider four features that manufacturers and suppliers should be able to provide.[3]

1. Coordinated vulnerability disclosure (CVD), often in the form of a vulnerability disclosure program (VDP)
2. Secure software updates
3. Software supply chain transparency, likely in the form of software bills of materials (SBOM)
4. Clarity about the duration of security support, related to end of life (EOL)

The Cybersecurity Best Practices for the Safety of Modern Vehicles Draft 2020 Update already addresses three of the four features. We appreciate and acknowledge the work performed by NHTSA to include these features that we consider to be important and effective contributions to security and safety.

1. Section *4.4 Security Vulnerability Reporting Program* discusses the reporting and sharing of vulnerability information.
2. Secure software updates are discussed in section *8.8 Software Updates / Modifications*.
3. Software supply chain transparency is covered in section *4.2.6 Inventory and Management of Software Assets on Vehicles*.
4. This leaves the feature concerning the duration of security support and end of life.

[2] We acknowledge that “hardware-only” vulnerabilities exist, however the causes of most vulnerabilities are rooted in software, often called firmware in embedded systems.
[3] We use the word “feature” more generally and in place of the specific terms “requirement,” “control,” “practice,” or “process.”

End of Security Support

Description

Software systems, and their upstream dependencies, have life cycles. At some point, software is no longer supported. This is often called the End of Life (EOL) date, although our specific concern is the date after which security updates will no longer be provided. An important part of managing vulnerabilities is knowing whether a software component is supported by the manufacturer or supplier, and whether or not security updates will be available.

Manufacturers and suppliers should provide dates after which software components and software systems will no longer receive security updates. This information should be provided as part of procurement between manufacturers and suppliers, and manufacturers should provide this information to customers, possibly as part of the Monroney sticker.

The Auto-ISAC notes that "...it takes an OEM approximately four years to develop a new product. A vehicle may then be in production for several years." Furthermore:

> Even after a vehicle is no longer in production, OEMs may support vehicle security for some extended period due to continued driver user [sic]. Average life expectancy for a passenger vehicle is 8 or more years, and for commercial vehicles, it can be much longer. Maintenance of security during this long period can be challenging.[4]

Providing end-of-life information is a common practice for more general purpose software, including operating systems. Google provides EOL information for Chrome devices[5] and D-Link acknowledges that certain vulnerable routers are unsupported and will not be updated for a remote command execution vulnerability.[6]

We do not recommend a specific period of security support, only that manufacturers and suppliers negotiate and declare a time period.

Suggested Implementation

We suggest adding an EOL feature within or immediately after section 4.2.6 Inventory and Management of Software Assets on Vehicles. EOL information is closely related to software assets. We provide the following draft text but defer to NHTSA as to whether, where, and how to implement the suggestion.

[G.12] Manufacturers and suppliers should advertise dates after which security support for motor vehicles and components will no longer be provided.

[4] Auto-ISAC Automotive Cybersecurity Best Practices Security Development Lifecycle, Version 1.3, Table 1
[5] https://support.google.com/chrome/a/answer/6220366
[6] https://kb.cert.org/vuls/id/766427