0 Day Discovery Report — Panasonic Head Unit 4G DNS Exfiltration

Author: Daniel C. Ulman (engaged by JDM System Consultants for FCA Chrysler)
Original discovery: November 2017

Confidentiality / Ownership
This finding was documented under a binding Non-Disclosure Agreement (NDA) between the involved parties. All proof-of-concept material, exploit-capable code, and related research remain confidential and are the property of FCA Chrysler in accordance with the NDA. AT&T assumed responsibility for remediation after coordinated disclosure.

Executive Summary

In November 2017, during a tightly scoped security evaluation of a Panasonic automotive head unit running QNX for FCA Chrysler, an issue was identified in the device's DNS handling that could allow data exfiltration through crafted DNS requests.

Access to protected `mmc` directories required a Panasonic Security Access Module (SAM). While reviewing network behavior, it was found that the head unit generated DNS queries without validating payload length or content, permitting arbitrary data to be embedded within outbound requests.

A controlled lab setup—emulating the head unit's IP address on AT&T's Jasper 4G network—demonstrated that the carrier's infrastructure accepted and forwarded these unfiltered queries. The behavior confirmed a viable channel for limited, covert data exfiltration. The issue was reported immediately to FCA and AT&T remediated within hours.

Scope & Context

- **Engagement:** Tightly scoped security assessment of Panasonic's QNX-based head unit on behalf of FCA Chrysler.
- **Platform:** Panasonic head unit, QNX OS; privileged access to the filesystem obtained via authorized SAM module.
- **Network:** Device connected to the AT&T 4G "Jasper" network.

Technical Findings

- Outgoing DNS queries lacked enforcement of payload size and character constraints, allowing arbitrary data to be embedded.
- AT&T’s network did not normalize or block such queries, enabling DNS to function as a covert exfiltration channel.
- The weakness arose from insecure DNS configuration and insufficient sanitization of data passed to the resolver.
- No memory-safety or privilege-escalation exploit was required—only logical misuse of the DNS protocol.

Additional Network Observation

Testing also revealed the contiguous IP block assigned to connected vehicles on the Jasper network. Controlled, authorized probes were performed against representative addresses in that range to confirm routability and validate that the head unit’s outbound DNS behavior was observable across those addresses. All interactions were non-destructive and limited to verifying the scope of network exposure and carrier handling of DNS traffic.

Proof of Concept (High-Level Summary)

- Access to the `mmc` directories via the SAM confirmed where DNS-related configuration resided.
- A controlled test host, impersonating the head unit’s IP, demonstrated that embedded-data DNS queries traversed the Jasper network and reached a monitored logging endpoint.
- Testing was strictly limited to verification of data flow; no destructive, persistent, or unauthorized actions were taken. All proof-of-concept artifacts remain under NDA.

Impact

- **Primary risk:** Exposure of sensitive device or telemetry data through covert DNS exfiltration.
- **Visibility:** Low; the traffic appeared as legitimate DNS queries.
- **Amplifying factor:** Carrier-side DNS forwarding that lacked payload normalization.

Remediation & Outcome

- The finding was reported immediately to FCA, AT&T, and Panasonic.
- The remediation was deployed within hours of notification.
- No public disclosure or exploit details were released.

Recommended Mitigation

1. Validate and sanitize all data inserted into DNS queries (length, character set, and format).
2. Prevent sensitive or user-specific data from being embedded in domain labels.
3. Apply query normalization or filtering at network egress and carrier gateways.
4. Implement monitoring for anomalous DNS patterns from connected devices.
5. Collaborate with carriers to establish controls against DNS-based data exfiltration.