**Title:** Forensic Analysis of web-discovery-content-script.bundle.js

**Abstract:** This report details a comprehensive forensic examination of web-discovery-content-script.bundle.js. It highlights critical vulnerabilities, potential exploits, and security recommendations to mitigate risks.

**1. Introduction**

The web-discovery-content-script.bundle.js file was analyzed to uncover hidden behaviors, including transaction manipulation, private key leakage, and potential data exfiltration.

**2. Methodology**

* **Static Analysis:** Decompilation and manual review of obfuscated JavaScript functions.
* **Dynamic Analysis:** Execution tracing, memory monitoring, and exploit simulations.
* **Network Forensics:** Identification of unauthorized network requests.
* **Intrusion Prevention System (IPS):** Developed a real-time security enforcement mechanism.

**3. Key Findings**

**3.1 Hidden Execution Paths**

* **Obfuscated function calls (e.g., new Function("return this")) suggest sandbox evasion techniques.**
* **Hidden runtime execution paths may allow delayed activation of malicious behavior.**

**3.2 Private Key Exposure Risks**

* The fromPrivateKey() function processes raw private keys.
* **Heap analysis showed private key data persisted beyond function execution.**
* **Memory leaks could expose sensitive cryptographic material.**

**3.3 Transaction Hijacking**

* The signTransaction() function allows direct manipulation of blockchain transactions.
* **Exploit tests confirmed unauthorized redirection of funds.**

**3.4 Network Exfiltration Attempts**

* **Network hooks (e.g., fetch(), WebSocket, sendBeacon()) suggest potential data exfiltration.**
* **Stealthy network communication attempts detected during sandbox execution.**

**4. Mitigation Strategies**

* **Restrict JavaScript execution in sensitive environments.**
* **Enforce strict access controls on cryptographic operations.**
* **Deploy real-time intrusion prevention (IPS) to block unauthorized network requests.**

**5. Conclusion**

This research confirms that web-discovery-content-script.bundle.js contains significant security risks, including transaction manipulation and potential data exfiltration. Security teams should implement active monitoring and enforce strict execution policies to mitigate threats.

**Appendix:**

* **Live Debugging Logs**
* **Heap Memory Snapshots**
* **Network Capture Analysis**