





Category: Technical Advisory

Technical Advisory – NXP i.MX SDP_READ_DISABLE Fuse Bypass (CVE-2022-45163)

Vendor: NXP Semiconductors Vendor URL: <https://www.nxp.com> Affected Devices: i.MX RT 101x, i.MX RT102x, i.MX RT1050/6x, i.MX 6 Family, i.MX 7 Family, i.MX8M Quad/Mini, Vybrid
Author: Jon Szymaniak <jon.szymaniak@nccgroup.com> CVE: CVE-2022-45163 Advisory URL: <https://community.nxp.com/t5/Known-Limitations-and-Guidelines/SDP-Read-Bypass-CVE-2022-45163/ta-p/1553565> Risk: 5.3 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N), 2.6 if C:L, 0.0 if C:N Summary NXP System-on-a-Chip (SoC) fuse configurations with the SDP_READ_REGISTER operation disabled (SDP_READ_DISABLE=1) ...

[Continue reading](#)

 Jon Szymaniak  Hardware & Embedded Systems, Research, Technical Advisory, Vulnerability
 November 17, 2022  12 Minutes

Technical Advisory – OpenJDK – Weak Parsing Logic in java.net.InetAddress and Related Classes

Vendor: OpenJDK Project Vendor URL: <https://openjdk.java.net> Versions affected: 8-17+ (and likely earlier versions) Systems Affected: All supported systems Author: Jeff Dileo <jeff.dileo@nccgroup.com> Advisory URL / CVE Identifier: TBD Risk: Low (implicit data validation bypass) Summary The private static InetAddress::getAllByName(String,InetAddress) method is used internally and by the public static InetAddress::getAllByName(String) to resolve host or IP strings ...

[Continue reading](#)

 Jeff Dileo  Research, Technical Advisory, Vulnerability  October 6, 2022  14 Minutes

Technical Advisory – Multiple Vulnerabilities in Juplink RX4-1800 WiFi Router (CVE-2022-37413, CVE-2022-37414)

Juplink's RX4-1800 WiFi router was found to have multiple vulnerabilities exposing its owners to potential intrusion in their local WiFi network and complete overtake of the device. An attacker can remotely take over a device after using a targeted or phishing attack to change the router's administrative password, effectively locking the owner out of their ...





[Continue reading](#)

 Jennifer Reed  Technical Advisory, Vulnerability  September 22, 2022  3 Minutes

There's Another Hole In Your SoC: Unisoc ROM Vulnerabilities

UNISOC (formerly Spreadtrum) is a rapidly growing semiconductor company that is nowadays focused on the Android entry-level smartphone market. While still a rare sight in the west, the company has nevertheless achieved impressive growth claiming 11% of the global smartphone application processor market, according to Counterpoint Research. Recently, it's been making its way into some ...





[Continue reading](#)

 Ilya Zhuravlev  Hardware & Embedded Systems, Technical Advisory, Vulnerability
 September 2, 2022  17 Minutes

Technical Advisory – Multiple vulnerabilities in Nuki smart locks (CVE-2022-32509, CVE-2022-32504, CVE-2022-32502, CVE-2022-32507, CVE-2022-32503, CVE-2022-32510, CVE-2022-32506, CVE-2022-32508, CVE-2022-32505)

The following vulnerabilities were found as part of a research project looking at the state of security of the different Nuki (smart lock) products. The main goal was to look for vulnerabilities which could affect to the availability, integrity or confidentiality of the different devices, from hardware to software. Eleven vulnerabilities were discovered. Below are ...





[Continue reading](#)

 Daniel Romero
 5G Security & Smart Environments, Hardware & Embedded Systems, Research, Technical Advisory, Vulnerability
 July 25, 2022  21 Minutes

Technical Advisory – ExpressLRS vulnerabilities allow for hijack of control link

Vendor: ExpressLRS Vendor URL: <https://expresslrs.org> Versions affected: 1.x, 2.x Author: Richard Appleby Severity: Medium 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Summary ExpressLRS is a high-performance open source radio control link. It aims to provide a low latency radio control link while also achieving maximum range. It runs on a wide variety of hardware in both 900 Mhz and 2.4 ...

[Continue reading](#)





 Richard Appleby  Emerging Technologies, Research, Technical Advisory, Vulnerability
 June 30, 2022  3 Minutes

Updated: Technical Advisory and Proofs of Concept – Multiple Vulnerabilities in U-Boot (CVE-2022-30790, CVE-2022-30552)

By Nicolas Bidron, and Nicolas Guigo. [Editor's note: This is an updated/expanded version of these advisories which we originally published on June 3 2022.] U-boot is a popular boot loader for embedded systems with implementations for a large number of architectures and prominent in most linux based embedded systems such as ChromeOS and Android Devices.

...





[Continue reading](#)

 Nicolas Bidron  Hardware & Embedded Systems, Technical Advisory, Vulnerability
 June 16, 2022  10 Minutes

Technical Advisory – Multiple Vulnerabilities in Trendnet TEW-831DR WiFi Router (CVE-2022-30325, CVE-2022-30326, CVE-2022-30327, CVE-2022-30328, CVE-2022-30329)

The Trendnet TEW-831DR WiFi Router was found to have multiple vulnerabilities exposing the owners of the router to potential intrusion of their local WiFi network and possible takeover of the device. Five vulnerabilities were discovered. Below are links to the associated technical advisories: Technical Advisory: Stored XSS in Web Interface for Trendnet TEW-831DR WiFi router ...





[Continue reading](#)

 Andrea Shirley-Bellande  Research, Technical Advisory, Vulnerability  June 10, 2022
 6 Minutes

Technical Advisory – Multiple Vulnerabilities in U-Boot (CVE-2022-30790, CVE-2022-30552)

By Nicolas Bidron, and Nicolas Guigo. U-boot is a popular boot loader for embedded systems with implementations for a large number of architectures and prominent in most Linux based embedded systems such as ChromeOS and Android Devices. Two vulnerabilities were uncovered in the IP Defragmentation algorithm implemented in U-Boot, with the associated technical advisories below: ...

[Continue reading](#)

 Nicolas Bidron  Hardware & Embedded Systems, Research, Technical Advisory, Vulnerability
 June 3, 2022  5 Minutes

Technical Advisory – FUJITSU CentricStor Control Center <= V8.1 – Unauthenticated Command Injection (CVE-2022-31794 and CVE-2022-31795)

On the 6th of April 2022, NCC Group's Fox-IT discovered two separate flaws in FUJITSU CentricStor Control Center V8.1 which allows an attacker to gain remote code execution on the appliance without prior authentication or authorization.

 Luke Paris  Technical Advisory, Vulnerability  May 27, 2022  3 Minutes