## Machine Learning 101: The Integrity of Image (Mis)Classification?

December 15, 2022 by Eric Schorn

Professor Ron Rivest observed the close relationship between cryptography and machine learning at the ASIACRYPT conference back in 1991. Cross-fertilization of common notions, such as integrity, privacy, confidentiality and authenticity, have only grown in the following three decades as these fields have become more central to our everyday lives. This blog post is the first in… Read more

## Replicating CVEs with KLEE

December 12, 2022 by nccmarktedman

This blog post details the steps taken to replicate a udhcpc process crash on BusyBox 1.24.2 using NVD – CVE-2016-2147 (nist.gov), and to produce a working denial of service exploit. We will be using the symbolic execution engine called KLEE to help identify parameters that can cause the specific crash we are interested in. This… Read more

## Public Report – VPN by Google One Security Assessment

December 9, 2022 by Daniel Romero

During the summer of 2022, Google engaged NCC Group to conduct a security assessment of VPN by Google One. VPN by Google One is a service that increases connection security and privacy to end users. Google provides several clients covering the most widely used operating systems; these VPN clients provide both encrypted transit and IP… Read more

## Public Report – Confidential Space Security Review

December 6, 2022 by Viktor Gazdag

During the summer of 2022, Google engaged NCC Group to conduct a security assessment of the Confidential Space product. The system provides a confidential computing environment that allows cloud customers to run workloads in the cloud that can be attested to run a specific payload with high assurances that the workload was not and cannot… Read more

## Exploring Prompt Injection Attacks

December 5, 2022 by Jose Selvi

Have you ever heard about Prompt Injection Attacks[1]? Prompt Injection is a new vulnerability that is affecting some AI/ML models and, in particular, certain types of language models using prompt-based learning.  This vulnerability was initially reported to OpenAI by Jon Cefalu (May 2022)[2] but it was kept in a responsible disclosure status until it was… Read more

## So long and thanks for all the 0day

November 23, 2022 by Jennifer Fernick

After nearly four years into my role, I am stepping down as NCC Group's SVP & Global Head of Research. In part just for myself, to reflect on a whirlwind few years, and in part as a thank you and celebration of all of the incredible researchers with whom I have had the privilege of… Read more

## A jq255 Elliptic Curve Specification, and a Retrospective

November 21, 2022 by Thomas Pornin

First things first: there is now a specification for the jq255e and jq255s elliptic curves; it is published on the C2SP initiative and is formally in (draft) version 0.0.1: https://github.com/C2SP/C2SP/blob/main/jq255.md The jq255e and jq255s groups are prime-order groups appropriate for building cryptographic protocols, and based on elliptic curves. These curves are from the large class… Read more

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

November 17, 2022 by Jon Szymaniak

Summary NXP System-on-a-Chip (SoC) fuse configurations with the SDP READ_REGISTER operation disabled (SDP_READ_DISABLE=1) but other serial download functionality still enabled (SDP_DISABLE=0) can be abused to read memory contents in warm and cold boot attack scenarios. In lieu of an enabled SDP READ_REGISTER operation, an attacker can use a series of timed SDP WRITE_DCD commands to… Read more

## Tool Release – Web3 Decoder Burp Suite Extension

November 10, 2022 by Mario Rivas

Web3 Decoder is a Burp Suite Extension that allows to decode "web3" JSON-RPC calls that interact with smart contracts in a EVM blockchain. As it is said that a picture is worth a thousand words, the following two screenshots shows a Raw JSON-RPC call, and its decoded function call: Background When auditing a DApp (Decentralized… Read more

## Tales of Windows detection opportunities for an implant framework

November 9, 2022 by Ollie Whitehouse

Slides from a fifteen minute lightening talk on detection opportunities for implant framework behaviour on Windows.

## Check out our new Microcorruption challenges!

October 31, 2022 by Jennifer Fernick

New Microcorruption challenges created by Nick Galloway and Davee Morgan Today we are releasing several new challenges for the embedded security CTF, Microcorruption. These challenges highlight types of vulnerabilities that NCC Group's Hardware and Embedded Systems practice have discovered in real products. The new challenges provide a simple interface to explore these vulnerabilities without having… Read more

## Toner Deaf – Printing your next persistence (Hexacon 2022)

October 17, 2022 by Alex Plaskett

On Friday 14th of October 2022 Alex Plaskett (@alexjplaskett) and Cedric Halbronn (@saidelike) presented Toner Deaf – Printing your next persistence at Hexacon 2022. This talk demonstrated remote over the network exploitation of a Lexmark printer and persistence across both firmware updates and reboots. The video from this talk is now available here: The slides… Read more

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

October 6, 2022 by Jeff Dileo

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[at]nccgroup[dot]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… Read more

## Public Report – IOV Labs powHSM Security Assessment

October 5, 2022 by Jennifer Fernick

In June 2022, IOV Labs engaged NCC Group to perform a review of powHSM. Per the project documentation: “Its main role is to safekeep and prevent the unauthorized usage of each of the powPeg’s members’ private keys. powHSM is implemented as a pair of applications for the Ledger Nano S, namely a UI and a Signer,… Read more

## Shining New Light on an Old ROM Vulnerability: Secure Boot Bypass via DCD and CSF Tampering on NXP i.MX Devices

October 3, 2022 by Jon Szymaniak

NXP’s HABv4 API documentation references a now-mitigated defect in ROM-resident High Assurance Boot (HAB) functionality present in devices with HAB version < 4.3.7. I could find no further public documentation on whether this constituted a vulnerability or an otherwise “uninteresting” errata item, so I analyzed it myself! This post shines new light on this old… Read more

View all posts