UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00070

PLATYPUS ATTACK STEALS DATA FROM INTEL CPUS

DATE ISSUED: 16th November 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

PLATYPUS serves as an acronym for Power Leakage Attacks Targeting Your Protected User Secrets. Discovered by a team of academic researchers. The Running Average Power Limit (RAPL) component that monitors power consumption in the CPU and DRAM is potentially able to be exploited by malicious actors.

BREAKDOWN

Graz University of Technology, the University of Birmingham and the CISPA Helmholtz Centre for Information Security have revealed that the readings taken from the RAPL component can be observed to determine activity carried out on a system. These fluctuations in power consumption can indicate the different Hamming weights of operands, instructions under execution, and memory loads revealing "loaded values," which is data loaded onto the CPU, to attackers. The values may include sensitive information such as passwords or encryption keys. Using PLATYPUS, an attacker can bypass internal security systems by using these power consumption values when examined for as little as 20 seconds. The PLATYPUS attack seems to be most effective when executed on Linux systems, based on the research at this stage. Attacks on Windows and Mac devices are made possible with the installation of the Intel Power Gadget application.

CVE-2020-8694 and CVE-2020-8695

REMEDIATION STEPS

- Backup data on all systems requiring updates
- Update systems according to normal testing and installation processes – see the latest advisory from Intel below for affected systems list and remediation actions

REFERENCES & RESOURCES

Intel:	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00389.html
ZDNet:	https://www.zdnet.com/article/new-platypus-attack-can-steal-data-from-intel-cpus/?ftag=TRE49e8aa0&bhid=29606343124056600886148366084033&mid=13161966&cid=2352480217