CVE-2020-6616

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-6616
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-08 20:15:00 UTC
Updated	2023-01-09 16:41:00 UTC
Description	Some Broadcom chips mishandle Bluetooth random-number generation because a low-entropy Pseudo Random Number C

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2018-002	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2018-003	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-001	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-002	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-003	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-007	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.13.6	supplemental_update	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-001	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-002	All	All

Operating System	Apple	Mac Os X	10.14.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-007	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update	All	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update_2	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All
Hardware	Samsung	Galaxy Note8	-	All	All	All
Hardware	Samsung	Galaxy Note8	-	All	All	All
Hardware	Samsung	Galaxy S8	-	All	All	All
Hardware	Samsung	Galaxy S8	-	All	All	All
Hardware	Samsung	Galaxy S8 Plus	-	All	All	All
Hardware	Samsung	Galaxy S8 Plus	-	All	All	All

References

Reference
media.ccc.de - Finding Eastereggs in Broadcom's Bluetooth Random Number Generator
Finding bugs in Bluetooth
Full Disclosure: APPLE-SA-2020-05-26-1 iOS 13.5 and iPadOS 13.5
About the security content of macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra - Apple Supp
Jiska on Twitter: "The Samsung Galaxy S8 Bluetooth chip is missing a hardware random number generator and the pseudo random number g
internalblue/rng.md at master · seemoo-lab/internalblue · GitHub
About the security content of iOS 13.5 and iPadOS 13.5 - Apple Support
About the security content of iOS 13.5 and iPadOS 13.5 - Apple Support
Samsung Mobile Security
Jiska on Twitter: "Broadcom did not provide us with any patches in advance, so we have no idea how they will fix this issue. Also, after our init
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.