2017. gada episkākas klupnes

Bernhards Blumbergs, CERT.LV

ETERNALBLUE

- CVE-2017-0143, MS17-010
- Datums: 14/04/2017
- Mērķis: MS Windows
- Ietekme: attālinātā koda izpilde
- Piekļuve: attālināta (datortīkls)
- Ievainojamība: kļūdas MS SMBv1 servisā
- Ielāps: pieejams

ETERNALBLUE@EsiDrošs

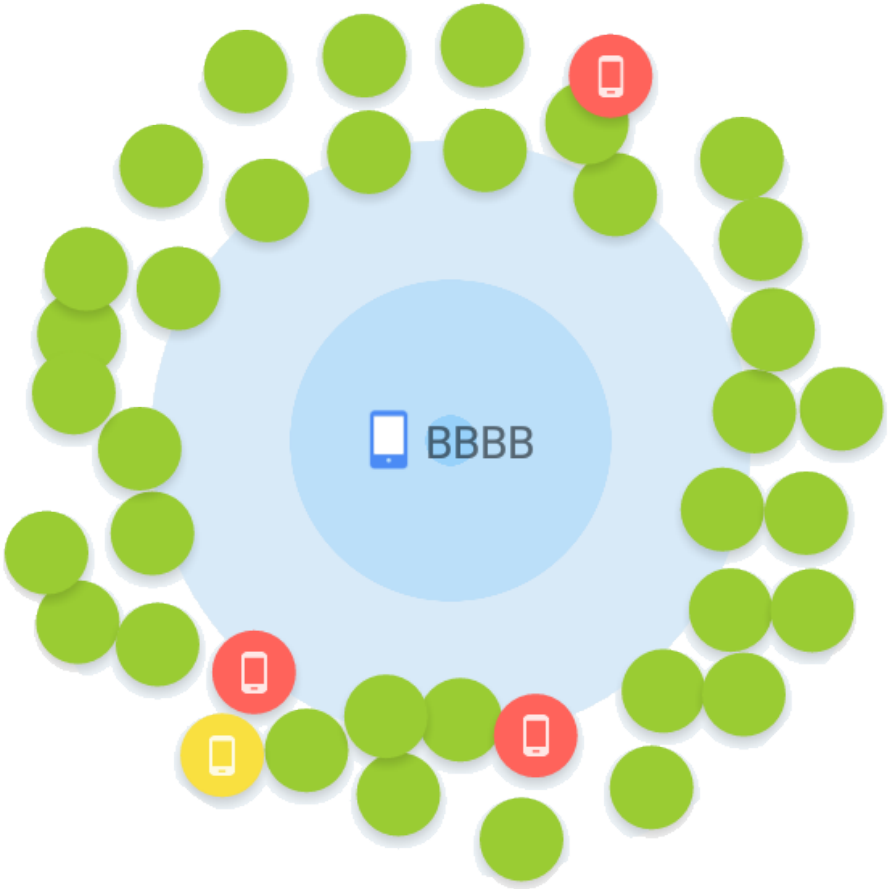
- WiFi “Citadele Free”

msf auxiliary(**smb_ms17_010**) > exploit
[-] 10.103.17.XXX:445 - Host does NOT appear vulnerable.
[*] Scanned 413 of 4096 hosts (10% complete)
[*] Scanned 824 of 4096 hosts (20% complete)
[*] Scanned 1235 of 4096 hosts (30% complete)
[-] 10.103.21.XXX:445 - Host does NOT appear vulnerable.
[*] Scanned 1639 of 4096 hosts (40% complete)
[*] Scanned 2062 of 4096 hosts (50% complete)
[*] Scanned 2462 of 4096 hosts (60% complete)
[*] Scanned 2877 of 4096 hosts (70% complete)
[*] Scanned 3294 of 4096 hosts (80% complete)
[*] Scanned 3694 of 4096 hosts (90% complete)
[*] Scanned 4096 of 4096 hosts (100% complete)
[*] Auxiliary module execution completed

BlueBorne

- CVE-2017-078[1-5]
- Datums: 13/09/2017
- Mērķis: Dažādu OS Bluetooth serviss
- Ietekme: pilna iekārtas kontrole
- Piekļuve: attālināta (bluetooth)
- Ievainojamība: vairākas kļūdas Bluetooth servisa protokolu kopnē
- Ielāps: pieejams - Apple, Google, Microsoft

BlueBorne@EsiDrošs



KRACK

- CVE-2017-130[77-82,84,86-88]
- Datums: 16/10/2017
- Mērķis: WiFi WPA2 drošības protokols
- Ietekme: pilna piekļuve WiFi kanālam
- Piekļuve: attālināta (WiFi)
- Ievainojamība: atkārtota WiFi kanāla šifra IV un atslēgas lietošana
- Ielāps: atkarībā no ražotāja

KRACK@EsiDrošs

SSID: Citadele Free

Bez paroles :)

:(

MacOS High Sierra fail

- CVE-2017-13872
- Datums: 28/11/2017
- Mērķis: MacOS High Sierra
- Ietekme: sistēmas (root) līmeņa piekļuve
- Piekļuve: fiziska
- Ievainojamība: root konta tukša parole un rakstāms crontab
- Ielāps: pieejams

Atsauces

- Microsoft Security Bulletin MS17-010 – Critical, https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
- Everything you need to know about EternalBlue – the NSA exploit linked to Petya, http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch
- The Attack Vector “BlueBorne” Exposes Almost Every Connected Device, https://www.armis.com/blueborne/
- Blueborne, the latest Bluetooth vulnerability, https://www.androidcentral.com/lets-talk-about-blueborne-latest-bluetooth-vulnerability
- Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse, https://www.krackattacks.com/
- KRACK - Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, https://www.youtube.com/watch?v=fOgJswt7nAc
- Apple About the security content of Security Update 2017-001, https://support.apple.com/en-us/HT208315
- Apple Announces Emergency Patch to Fix High Sierra Login Bug, https://threatpost.com/apple-announces-emergency-patch-to-fix-high-sierra-login-bug/129039/
- macOS High Sierra 10.13.1 insecure cron system, http://seclists.org/fulldisclosure/2017/Dec/25