A MICROSOFT GÖRBE ESTÉJE

MIT TANULHATUNK A PWNIE-DÍJJAL JUTALMAZOTT CVE-2020-0601-BŐL

Veres-Szentkirályi András 2021-01-16

$ whoami

Veres-Szentkirályi András

- OSCP, GWAPT, SISE
- Silent Signal alapító
- pentester, toolmaker

Menetrend

1. Bevezetés
2. CVE-2020-0601
3. Zoom out

Végre kriptográfiára is ellőhetem

silent signal

“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break.”

– Bruce Schneier (1998. október 15.)
https://www.schneier.com/crypto-gram-9810.html#cipherdesign

Pwnie awards

silent signal

Menetrend

1. Bevezetés
2. CVE-2020-0601
3. Zoom out

Pwnie awards – Most Epic Fail 2020

silent signal

This award is for the defenders who dared to wonder, “What could possibly go wrong?” For the investors who happily departed with eight-figure checks for a pitch presenting snake oil served over word salads on a fool’s gold platter. For the infosec vendors who adopted defense-by-deception as a marketing strategy. This award will honor a person or corporate entity’s spectacularly epic fail – the kind of fail that lets the entire infosec industry down in its wake. It can be a singular incident, marketing piece, or investment – or a smoldering trail of whale-scale fail. Microsoft

Microsoft’s implementation of elliptic curve signatures allowed attackers to generate private pairs for the public keys of any legitimate signer. This enabled spoofing of any HTTPS website or signed binary on affected versions of Windows. We wish Microsoft was as lenient when choosing the time of updates, as it was for choosing generator points!

Olvasnivaló

silent signal

- https://news.ycombinator.com/item?id=22048619
- https://medium.com/zengo/win10-crypto-vulnerability-cheating-in-elliptic-curve-billiards-2-69b45f2dcab6
- https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/blocking-a-curveball-pocs-out-for-critical-microsoft-nsa-bug-cve-2020-0601
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601
- https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF
- https://www.trendmicro.com/en_us/research/20/a/january-patch-tuesday-update-list-includes-fixes-for-internet-explorer-remote-desktop-crypto
  html
- https://www.trendmicro.com/en_us/research/20/b/an-in-depth-technical-analysis-of-curveball-cve-2020-0601.html

Kapcsolódó

silent signal

- 2018-as Pwnies crypto kategória jelöltjeinek bemutatása – Budapest New Tech Meetup
  `https://www.youtube.com/watch?v=v_jbzmfgHkQ`
- 2020.09.12. Elliptikus görbékről bevezető – Online Meetup
  `https://www.youtube.com/watch?v=YKWphlmm2G8#t=929s`
- 2020.07.25. Kriptográfiai alapok fejlesztőknek és érdeklődőknek – Online Meetup
  `https://www.youtube.com/watch?v=XSIy8gmjmgY#t=4343s`

PKI

silent signal

- CA: aláír egy publikus kulcs + identitás párost
- tanúsítvánnyal ellenőrizhető(?) az aláíró kiléte
- mindez sorosan kapcsolva: bármi bugos, a támadó nyer
- mit sem ér az erős elem, ha a leggyengébb láncszem törhető
  - `https://buhera.blog.hu/2014/02/22/apple_vs_ssl_goto_fail`
  - `https://buhera.blog.hu/2014/03/04/gnutls_vs_ssl_goto_cleanup`

PKI + ECDSA

silent signal

- minden EC-hez tartozik egy p, standard a G bázispont
- privát kulcs: k skalár $\bmod p$
- publikus kulcs: kG – könnyen számolható, nehezen visszafejthető
- t.f.h. van egy valid tanúsítványunk, publikus kulcsa $Q = xG$
- x-et nehéz lenne kipörgetni

PKI + ECDSA

silent signal

- minden EC-hez tartozik egy p, standard a G bázispont
- privát kulcs: k skalár mod$p$
- publikus kulcs: kG – könnyen számolható, nehezen visszafejthető
- t.f.h. van egy valid tanúsítványunk, publikus kulcsa $Q = xG$
- x-et nehéz lenne kipörgetni
- ha viszont a támadó adhat saját bázispont, $Q = x'G'$ könnyebben számítható
- pofátlan mód: $x' = 1$ és $G' = Q$

Menetrend

1. Bevezetés
2. CVE-2020-0601
3. Zoom out

CVE-2020-0601 részletesen

silent signal

- X.509: szabvány tanúsítványokra ASN.1 alapokon
- Tanúsítvány » Subject Public Key Info » Algoritmus » EC paraméterek
- lehetőségek: „nevesített” görbe (pl. P-256) vs. saját paraméterek (lásd $G' = Q$)
- Microsoft CryptoAPI: csak a publikus kulcs (Q) alapján keres a megbízható CA-k tárában, nem nézi a görbe név/paraméter (G és társai) szerinti egyezőséget
- NSA: “Certificates containing **explicitly-defined elliptic curve parameters** which only partially match a standard curve **are suspicious**, especially if they include the public key for a trusted certificate, **and may represent bona fide exploitation attempts**.”

Root cause analysis helyett

silent signal

- alapprobléma: két dologról feltételezzük, hogy ekvivalensek $\Rightarrow$ bármelyiket felhasználhatjuk
- defense in depth/hardening: jobb a megbízhatóbbat használni a kettő közül

Root cause analysis helyett

silent signal

- alapprobléma: két dologról feltételezzük, hogy ekvivalensek $\Rightarrow$ bármelyiket felhasználhatjuk
- defense in depth/hardening: jobb a megbízhatóbbat használni a kettő közül
- Szerencsére ilyet csak a Microsoft csinálhat, ugye?

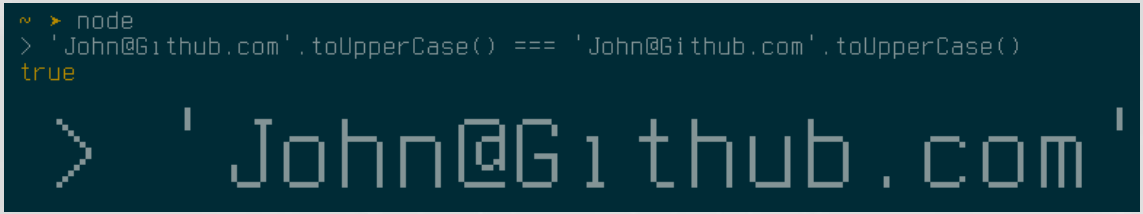
GitHub elfelejtett jelszó (2019. nov.)

silent signal

```
~ ➤ node
> 'John@Gıthub.com'.toUpperCase() === 'John@Github.com'.toUpperCase()
true
> 'John@Gıthub.com'
```

- Blog post további érdekes karakterekkel:
  `https://eng.getwisdom.io/hacking-github-with-unicode-dotless-i/`
- Django reakciója:
  `https://www.djangoproject.com/weblog/2019/dec/18/security-releases/`

GitHub elfelejtett jelszó (2019. nov.)



- Blog post további érdekes karakterekkel:
  `https://eng.getwisdom.io/hacking-github-with-unicode-dotless-i/`
- Django reakciója:
  `https://www.djangoproject.com/weblog/2019/dec/18/security-releases/`
- Szerencsére ilyen csak zárt forrású szoftverben lehetséges, ugye?

Let's Encrypt (2015. aug.)

silent signal

- `https://www.agwa.name/blog/post/duplicate_signature_key_selection_attack_in_lets_encrypt`
- The vulnerability was caused by a misuse of digital signatures. The guarantee provided by digital signatures is the following:
  - Given a message, a signature, and a public key, a valid digital signature tells you that the message was authored by the holder of the corresponding private key.
- Digital signatures guarantee that **a message came from a particular private key**. They do **not** guarantee that **a signature came from a particular private key**, and with RSA it's **quite easy** to find a private key that produces a desired signature for a particular message.

Matekozzunk!

silent signal

- $s = m^d \pmod{n}$ – m üzenetet d privát kulccsal aláírtuk $\Rightarrow$ létrejött az s aláírás
- Feladat: e, d és n értékeket keresni, amire $s^e = m \pmod{n}$
- RSA miatt tudjuk, hogy tetszőleges x értékre $(x^d)^e = x \pmod{n}$
- Triviális megoldás: $e = d = 1, n = s - m \Rightarrow$ utóbbit teljesíti
- Feladat is teljesíti: $s = m \pmod{s - m} \iff \text{s - m} = 0 \pmod{s - m} \iff 0 = 0 \pmod{s - m}$

"This produces a highly implausible RSA key pair. …However, **not all RSA implementations are picky** with these details. For example, **Go's RSA implementation happily validates such signatures** (Let's Encrypt's backend is written in Go). Note that this is in not a bug in Go, since these details don't matter when signatures are used properly."

"ACME has been redesigned so that a hash of the ACME account public key (plus a random token) is published in the DNS instead of a signature. The old challenges were disabled on November 19, 2015."

Összefoglalás

silent signal

- kriptográfiai primitívekkel dolgozni veszélyes szakma
- ha két dolog elvileg azonos, dolgozzunk a megbízhatóbb változattal
- mit sem ér az erős elem, ha a leggyengébb láncszem törhető

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal