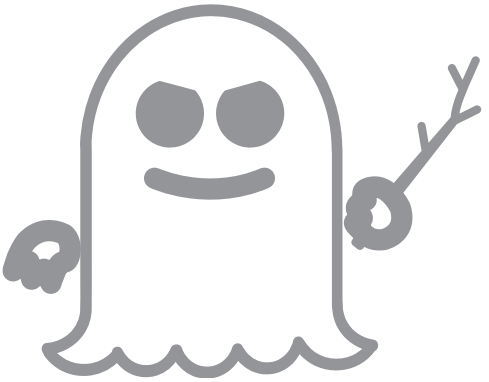
Mimo wszystko fenomen brandowanych błędów jest zjawiskiem ciekawym i pozytywnym. Wprowadza również ferment i pewną dozę humoru do hermetycznego światka bezpieczeństwa.

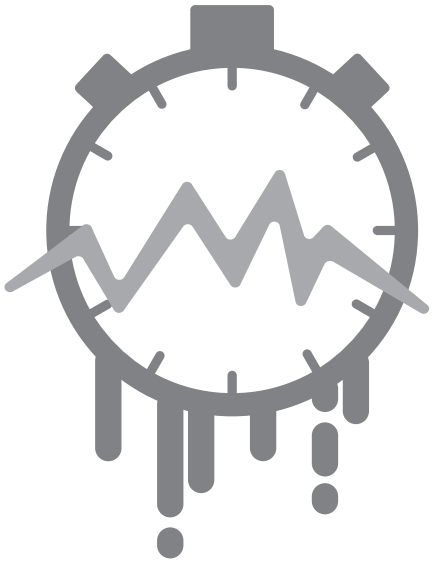
Innymi ciekawszymi brandowanymi błędami, które warto tu wymienić, były Shellshock (CVE-2014-6271; jak się okazało bardzo powszechna i łatwa do wykorzystania podatność w wielu systemach; logo na rysunku 2.2)[18] czy Spectre (CVE-2017-5753, CVE-2017-5715; klasa rodzajów błędów atakujących mikroarchitektury procesorów, zatem nie jest to błąd w oprogramowaniu; logo na rysunku 2.3) lub Hertzbleed (CVE-2022-23823, CVE-2022-24436; logo tego błędu na poziomie procesora jest na rysunku 2.4).

Rys. 2.2. Logo Shellshock (CVE-2014-6271)
Źródło: https://openclipart.org/detail/202368/shellshock-bug.



Rys. 2.3. Logo Spectre (CVE-2017-5753, CVE-2017-5715)
Źródło: https://meltdownattack.com.

[18] W wyniku przetwarzania specjalnie stworzonych danych wejściowych (np. zawierających "() { :;}; /bin/cat /etc/passwd") „parser" oprogramowania gdzieś dosięgał ostatecznie powłoki Bash, która następnie wykonywała żądane polecenie. Mogło to doprowadzić do wykradania danych i przejęcia kontroli nad systemami.



Rys. 2.4. Logo Hertzbleed (CVE-2022-23823, CVE-2022-24436)
Źródło: https://www.hertzbleed.com/.

Technika ta jest bardzo ciekawa i pomocna zwłaszcza w wypadku takich właśnie błędów – szeroko rozpowszechnionych, być może stosunkowo łatwych do wykorzystania (jak Heartbleed lub Shellshock), aż proszących się o jak najszybsze rozwiązanie problemu. W pewnym sensie również spektakularnych. W innych kontekstach: logotyp powstaje, gdyż jest to fajne.

2.9.1. 20-letnie błędy w zabezpieczeniach?

Jako ciekawostkę dodajmy, że niektóre podatności bezpieczeństwa istniały w oprogramowaniu nawet przez 10[19] czy 20[20] lat. Tyle czasu zajęło ich znalezienie, zidentyfikowanie, a następnie poprawienie. Wobec tak długiego czasu życia niektórzy czasem zastanawiają się nad hipotetycznymi konsekwencjami. Co, jeśli ktoś inny znalazł taki 20-letni błąd[21] powiedzmy 10 lat temu? Wtedy mógłby hakować systemy przez całe 10 lat! Nie do końca tak jest, bo wydaje się, że dzięki zasobom poświęconym na monitorowanie systemów prędzej czy później wykorzystanie jakichś nieznanych luk zostałoby wykryte i poddane śledztwu. Wtedy te „jakieś nieznane" luki być może zostałyby zidentyfikowane jako „bardzo konkretne" luki. Choć oczywiście nie można wykluczyć, że ktoś lub coś faktycznie wykorzystywało podatności w oprogramowaniu przez tak długie lata. Trzeba bowiem przyznać, że 20 lat temu standardy

[19] CVE-2021-3156 (2021), https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156.
[20] CVE-2019-1162 (2019), https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1162.
[21] European Commission, *20-year-old open source bug found and fixed under the EU-FOSSA 2 project*, 11.12.2019, https://ec.europa.eu/info/news/20-year-old-open-source-bug-found-and-fixed-under-eu-fossa-2-project-2019-dec-11_en.