0day "In the Wild"

Introduction | All | 2019 | 2018 | 2017 | 2016 | 2015 | 2014

	A
1	**0day "In the Wild"**
2	Last updated: 2019-05-15
3	
4	This spreadsheet is used to track cases of zero-day exploits that were detected "in the wild". This means the vulnerability was detected in real attacks against users as a zero-day vulnerability (i.e. not known to the public or the vendor at the time of detection). This data is collected from a range of public sources. We include relevant links to third-party analysis and attribution, but we do this only for your information; their inclusion does not mean we endorse or validate the content there.
5	
6	A detailed introduction to this spreadsheet is available on the Project Zero blog.
7	
8	Some additional notes on how the data is processed:
9	**- Scope for inclusion:** there are some 0day exploits (such as CVE-2017-12824) in areas that aren't active research targets for Project Zero. Generally this list includes targets that Project Zero has previously investigated (i.e. there are bug reports in our issue tracker) or will investigate in the near future.
10	**- Security supported:** this list does not include exploits for software that is explicitly EOL at the time of discovery (such as the ExplodingCan exploit for IIS on Windows Server 2003, surfaced in 2017).
11	**- Post-disclosure:** this list does not include CVEs that were opportunistically exploited by attackers in the gap between public disclosure (or "full disclosure") and a patch becoming available to users (such as CVE-2015-0072, CVE-2018-8414 or CVE-2018-8440).
12	**- Reasonable inference:** this list includes exploits that were not discovered in an active breach, but were leaked or discovered in a form that suggests with high confidence that they were probably used "in the wild" at some point (e.g. Equation Group and Hacking Team leaks).
13	**- Date resolution:** we only set the date of discovery when the reporter specifies one. If a discovery is indicated as being made in "late April" or "early March", we record that as if no date was provided.
14	**- Attribution:** generally the “claimed attribution” column refers to the attack team that is reportedly using the exploit, but in some cases it can refer to the supplier of the exploit (c.f. HackingTeam, NSO Group, Exodus Intel) if no other information is available.
15	**- Time range:** data collection starts from the day we announced Project Zero -- July 15, 2014.
16	
17	For additions, corrections, questions, or comments, please contact 0day-in-the-wild@google.com