Threat Analysis Group

Protecting Android users from 0-Day attacks

May 19, 2022

4 min read

Share Twitter Facebook Linkedin Mail Copy link C Clement Lecigne Threat Analysis Group C Christian Resell Threat Analysis Group Share Twitter Facebook Linkedin Mail Copy link

To protect our users, Google's Threat Analysis Group (TAG) routinely hunts for 0-day vulnerabilities exploited in-the-wild. In 2021, we reported nine 0-days affecting Chrome, Android, Apple and Microsoft, leading to patches to protect users from these attacks.

This blog is a follow up to our July 2021 post on four 0-day vulnerabilities we discovered in 2021, and details campaigns targeting Android users with five distinct 0-day vulnerabilities:

- CVE-2021-37973, CVE-2021-37976, CVE-2021-38000, CVE-2021-38003 in Chrome
- CVE-2021-1048 in Android

We assess with high confidence that these exploits were packaged by a single commercial surveillance company, Cytrox, and sold to different government-backed actors who used them in at least the three campaigns discussed below. Consistent with findings from CitizenLab, we assess government-backed actors purchasing these exploits are located (at least) in Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain and Indonesia.

The 0-day exploits were used alongside n-day exploits as the developers took advantage of the time difference between when some critical bugs were patched but not flagged as security issues and when these patches were fully deployed across the Android ecosystem. Our findings underscore the extent to which commercial surveillance vendors have proliferated capabilities historically only used by governments with the technical expertise to develop and operationalize exploits.

Seven of the nine 0-days TAG discovered in 2021 fall into this category: developed by commercial providers and sold to and used by government-backed actors. TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors.

Campaign Deep Dives

All three campaigns delivered one-time links mimicking URL shortener services to the targeted Android users via email. The campaigns were limited — in each case, we assess the number of targets was in the tens of users. Once clicked, the link redirected the target to an attacker-owned domain that delivered the exploits before redirecting the browser to a legitimate website. If the link was not active, the user was redirected directly to a legitimate website. We've seen this technique used against journalists and other unidentified targets, and alerted those users when possible.

We assess that these campaigns delivered ALIEN, a simple Android malware in charge of loading PREDATOR, an Android implant described by CitizenLab in December 2021. ALIEN lives inside multiple privileged processes and receives commands from PREDATOR over IPC. These commands include recording audio, adding CA certificates, and hiding apps.

Campaign #1 - redirecting to SBrowser from Chrome (CVE-2021-38000)

The first campaign, detected in August 2021, used Chrome on a Samsung Galaxy S21 and the web server immediately replied with a HTTP redirect (302) pointing to the following intent URL. This URL abused a logic flaw and forced Chrome to load another URL in the Samsung Browser without user interaction or warnings.

We did not capture the subsequent stages, but assess the attackers did not have exploits for the current version of Chrome (91.0.4472) at that time, but instead used n-day exploits targeting Samsung Browser, which was running an older and vulnerable version of Chromium.

We assess with high confidence this vulnerability was sold by an exploit broker and probably abused by more than one surveillance vendor.

More technical details about this vulnerability are available in this RCA by Maddie Stone.

```
intent://<URL>#Intent;scheme=https;package=com.sec.android.app.sbrowser;S.browser_fallback_u
rl=<EXPLOIT_URL>;end
```

Related IOCs

- s.bit-li[.]com - landing page
- getupdatesnow[.]xyz - exploit delivery server

Campaign #2 - Chrome sandbox escape (CVE-2021-37973, CVE-2021-37976)

In September 2021, TAG detected a campaign where the exploit chain was delivered to a fully up-to-date Samsung Galaxy S10 running the latest version of Chrome. We recovered the exploit used to escape the Chrome Sandbox, but not the initial RCE exploit.

The sandbox escape was loaded directly as an ELF binary embedding libchrome.so and a custom libmojo_bridge.so was used to ease the communication with the Mojo IPCs. This means the renderer exploit did not enable MojoJS bindings like we often see in public exploits.

Analysis of the exploit identified two different vulnerabilities in Chrome:

- CVE-2021-37973: A use-after-free in the handling of Portals API and Fenced subframes.
- CVE-2021-37976: An information leak in memory_instrumentation.mojom.Coordinator where Global Memory Dumps can be acquired for privileged processes. These dumps include sensitive information (addresses) which can be used for ASLR bypass.

After escaping the sandbox, the exploit downloaded another exploit in /data/data/com.android.chrome/p.so to elevate privileges and install the implant. We haven't retrieved a copy of the exploit.

Related IOCs

- shorten[.]fi - landing page
- contents-domain[.]com - exploit delivery and C2 server

Campaign #3 - Full Android 0-day exploit chain (CVE-2021-38003, CVE-2021-1048)

In October 2021, we detected a full chain exploit from an up-to-date Samsung phone running the latest version of Chrome.

The chain included two 0-day exploits:

- CVE-2021-38003: A Chrome renderer 0-day in JSON.stringify allowing the attacker to leak TheHole value and fully compromise the renderer.
- CVE-2021-1048: Unlike the previous campaign, the sandbox escape used a Linux kernel bug in the epoll() system call. This system call is reachable from the BPF sandbox and allows the attacker to escape the sandbox and compromise the system by injecting code into privileged processes. More information can be found in this RCA by Jann Horn.

Of note, CVE-2021-1048 was fixed in the Linux kernel in September 2020, over a year before this campaign. The commit was not flagged as a security issue and therefore the patch was not backported in most Android kernels. At the time of the exploit, all Samsung kernels were vulnerable; LTS kernels running on Pixel phones were recent enough and included the fix for this bug. Unfortunately, this is not the first time we have seen this happen with exploits in the wild; the 2019 Bad Binder vulnerability is another example. In both cases, the fix was not flagged as a security issue and thus not backported to all (or any) Android kernels. Attackers are actively looking for and profiting from such slowly-fixed vulnerabilities.

author	Al Viro <viro@zeniv.linux.org.uk>	2020-09-02 11:30:48 -0400
committer	Al Viro <viro@zeniv.linux.org.uk>	2020-09-02 11:30:48 -0400
commit	77f4689de17c0887775bb77896f4cc11a39bf848 (patch)	
tree	48e71e89ec43f9869327fc81f1b8c83ffb60c72d	
parent	52c479697c9b73f628140dcdfcd39ea302d05482 (diff)	
download	linux-77f4689de17c0887775bb77896f4cc11a39bf848.tar.gz	

fix regression in "epoll: Keep a reference on files added to the check list"

```
epoll_loop_check_proc() can run into a file already committed to destruction;
we can't grab a reference on those and don't need to add them to the set for
reverse path check anyway.

Tested-by: Marc Zyngier <maz@kernel.org>
Fixes: a9ed4a6560b8 ("epoll: Keep a reference on files added to the check list")
Signed-off-by: Al Viro <viro@zeniv.linux.org.uk>
```

Related IOCs

- shorten[.]fi - landing page
- redirecting[.]page - exploit delivery and C2 server
- 8e4edb1e07ebb86784f65dccb14ab71dfd72f2be1203765b85461e65b7ed69c6 - ALIEN

Conclusion

We'd be remiss if we did not acknowledge the quick response and patching of these vulnerabilities by Google's Chrome and Android teams. We would also like to thank Project Zero for their technical assistance in helping analyze these bugs. TAG continues to track more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors. We remain committed to updating the community as we uncover these campaigns.

Tackling the harmful practices of the commercial surveillance industry will require a robust, comprehensive approach that includes cooperation among threat intelligence teams, network defenders, academic researchers and technology platforms. We look forward to continuing our work in this space and advancing the safety and security of our users around the world.

POSTED IN: