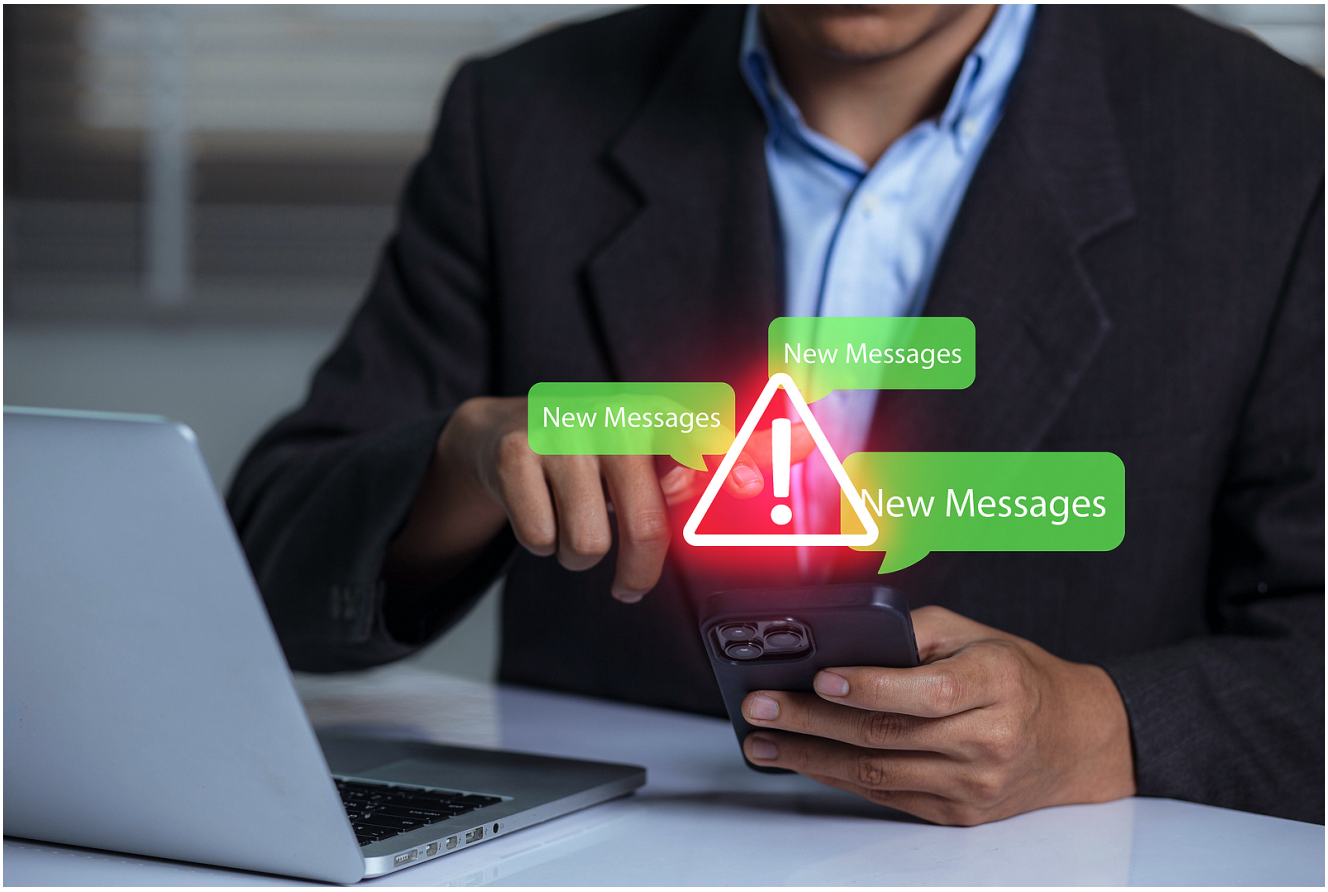
Google Links More iOS, Android Zero-Day Exploits to Spyware Vendors



Several zero-day vulnerabilities patched last year had been exploited by commercial spyware vendors to target Android and iOS devices, according to a report published on Wednesday by Google's Threat Analysis Group (TAG).

Google's security researchers have detailed the zero-day and n-day vulnerabilities exploited in what they described as two different highly targeted campaigns. For many of the zero-days, no information was available until now on the attacks exploiting them.

The internet giant has been tracking more than 30 spyware vendors that provide exploits and surveillance solutions to governments. While the surveillance technologies themselves

may not be illegal – they are typically advertised as solutions designed for official intelligence and law enforcement operations – the problem is that they are often used by governments to target the opposition, journalists, and dissidents.

In one of the two campaigns described by Google on Wednesday, an attack started with a link being sent to the targeted user via SMS. When clicked, the link took the victim to malicious websites delivering Android or iOS exploits – depending on the target's device. Once the exploits were delivered, victims were redirected to legitimate websites, likely in an effort to avoid raising suspicion.

The iOS exploit chain involved CVE-2022-42856, a WebKit vulnerability that Apple patched in iPhones in December 2022 with an iOS update. Attacks also involved a Pointer Authentication (PAC) bypass technique, and an exploit for CVE-2021-30900, a sandbox escape and privilege escalation vulnerability that Apple patched in iOS in 2021.

The Android exploit chain targeted CVE-2022-3723, a Chrome zero-day fixed by Google in October 2022.

It also targeted CVE-2022-4135, a Chrome flaw that Google patched in November 2022 – it was the eighth Chrome zero-day of 2022. This is a Chrome GPU sandbox bypass that only impacts Android devices.

The Android chain also included exploitation of CVE-2022-38181, an Arm Mali GPU vulnerability leading to arbitrary kernel code execution and root on Pixel 6 phones. A patch was released by Arm in August 2022, but it was only rolled out to Pixel devices in January 2023.

"When Arm released a fix for CVE-2022-38181, several vendors, including Pixel, Samsung, Xiaomi, Oppo and others, did not incorporate the patch, resulting in a situation where attackers were able to freely exploit the bug for several

months," Google said, noting that it's unclear if attackers had been exploiting the flaw before it was responsibly disclosed to Arm.

This campaign targeted users in Italy, Malaysia and Kazakhstan.

Google reported last year that Apple and Android smartphones in Italy and Kazakhstan had been targeted using spyware made by Italian company RCS Lab. However, Google noted in its new blog post that one of the techniques used against iOS devices has also been leveraged by the Predator spyware, made by North Macedonian spyware vendor Cytrox.

In the second campaign, discovered in December 2022, the attackers targeted the Samsung Internet Browser by chaining various zero-day and n-day vulnerabilities.

In this campaign as well, the exploits were delivered as links sent via SMS. The attacks were aimed at users in the United Arab Emirates and the goal was the delivery of full-featured Android spyware.

Google believes the attack was carried out by a customer or partner of Variston, a Spanish commercial spyware vendor whose exploitation frameworks were described by the internet giant last year.

The attackers exploited several Chrome vulnerabilities. The Samsung browser is based on Chromium, which means it's impacted by the same flaws as Chrome. However, the Samsung browser does not include some mitigations that would have made exploitation more difficult.

The list of exploits included CVE-2022-4262, a Chrome zero-day fixed by Google in December 2022, and CVE-2022-3038, a Chrome sandbox escape.

The campaign also targeted CVE-2022-22706, a Mali GPU kernel

driver issue fixed by Arm in January 2022, and CVE-2023-0266, a Linux kernel sound subsystem flaw that gives the attacker kernel read and write access. Both of these vulnerabilities were exploited in the wild against Android devices before patches were released.

Google has made available indicators of compromise (IoCs) that can be used to detect these attacks.

Related: Google Reveals Spyware Vendor’s Use of Samsung Phone Zero-Day Exploits

Related: US to Adopt New Restrictions on Using Commercial Spyware

Related: Leaked Docs Show Spyware Firm Offering iOS, Android Hacking Services for $8 Million

Google Links More iOS, Android Zero-Day Exploits to Spyware Vendors