

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Cyberwarfare](#)



Google Android Security Update Patches 40 Vulnerabilities

By [Ionut Arghire](#) on September 08, 2021

Share [Tweet](#)



Google on Tuesday published the Android Security Bulletin for September 2021 with patches for a total of 40 vulnerabilities, including seven that are rated critical.

A total of 16 issues were patched with the first part of this month's security updates - the 2021-09-01 security patch level - including one critical issue in the Framework component. Tracked as CVE-2021-0687, the security bug affects Android 8.1, 9, 10, and 11.

"The most severe of these issues is a critical security vulnerability in the Framework component that could enable a remote attacker using a specially crafted file to cause a permanent denial of service," according to [Google's advisory](#).

Six other vulnerabilities were patched in the Framework component, all considered high-severity. These include five elevation of privilege flaws and one information disclosure vulnerability.

Google also released patches for two high severity information disclosure issues in Media framework, and seven vulnerabilities in the System component: six high severity (two elevation of privilege and four information disclosure bugs) and one medium severity (elevation of privilege).

[READ: [Microsoft Office Zero-Day Hit in Targeted Attacks](#)]

This month's Android patches also include a Google Play system update to address the CVE-2021-0690 vulnerability.

The second part of September 2021's set of patches arrives on devices as the 2021-09-05 security patch level and includes fixes for a total of 23 vulnerabilities in Kernel components, MediaTek components, Unisoc components, Qualcomm components, and Qualcomm closed-source components.

Seven of these security holes, all of them addressed in Qualcomm closed-source components, are rated critical.

Google also announced [patches Pixel devices](#) address a total of nine other vulnerabilities, in Kernel, Pixel components, Qualcomm components, and Qualcomm closed-source components.

Pixel devices running a security patch level of 2021-09-05 or later have been patched for all of these issues, as well as for the vulnerabilities in the September 2021 Android Security Bulletin.

Related: [Google Patches High-Risk Android Security Flaws](#)

Related: [Google Details New Privacy and Security Policies for Android Apps](#)

 view counter

Share [Tweet](#)



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[US Gov Seeks Public Feedback on Draft Federal Zero Trust Strategy](#)

[Canadian-US National Sentenced to Prison for Cybercrime Schemes](#)

[Microsoft Warns of Information Leak Flaw in Azure Container Instances](#)

[Zoho Confirms Zero-Day Authentication Bypass Attacks](#)

[Howard University Cancels Classes, Shuts Campus After Ransomware Attack](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

 view counter

[2021 Singapore/APAC ICS Cyber Security Conference \[Virtual: June 22-24\]](#)

 view counter

[2021 CISO Forum: September 21-22 - A Virtual Event](#)

 view counter

[2021 ICS Cyber Security Conference | USA \[Hybrid: Oct. 25-28\]](#)

 view counter

 **Tags:**

[Cyberwarfare](#) [Disaster Recovery](#) [Endpoint Security](#) [Mobile Security](#) [NEWS & INDUSTRY](#) [Privacy](#) [Email Security](#) [Fraud & Identity Theft](#) [Incident Response](#) [Wireless Security](#) [Identity & Access](#) [Phishing](#) [Risk Management](#) [Virus & Malware](#) [Cloud Security](#) [Malware](#) [Vulnerabilities](#) [Data Protection](#)

Search

Get the Daily Briefing