unc0ver iOS Jailbreak

Overview

Unc0ver is a widely used jailbreak that has been present in the market for some time, and more recently started taking advantage of an iOS kernel vulnerability discovered in 2019. It can be installed on iOS devices from Windows, Linux, or macOS machines. Unc0ver supports iOS 11.0 through iOS 13.5 with the exception of 12.3-12.3.1 and 12.4.2-12.4.5. This makes it widely consumable and means that even the newest devices such as the iPhone 11, 2020 iPad Pro, and iPhone SE can all be jailbroken using unc0ver. Lookout can detect unc0ver and protect organizations against it.

How Does it Work?

Like other jailbreaks, unc0ver takes advantage of a vulnerability in the device's operating system to enable the user to have more control over the device than is normally allowed by the manufacturer. From a macOS, Windows, Linux, or iOS device, the user only has to follow a few basic steps in order to download the necessary tools to support the mobile jailbreak and have full access to their iOS device with the native iOS security and protections lifted. Everything to support this process is open-source and accessible on unc0ver's website, GitHub, and other sources, making it widely available. Once the jailbreak is complete it installs Cydia, a 3rd-party app store, and its pre-configured app repositories to the device.

Lookout Recommendation for Admins

Lookout Mobile Endpoint Security has a default policy to alert the device user and the organization's Lookout admin when a device is jailbroken. Lookout also covers Android devices being rooted, which is key for any organization running both iOS and Android devices in their mobile fleet.

Since a jailbreak for iOS or rooting for Android can lift many native protections and restrictions on a device, jailbreaking/rooting should be prohibited as part of an organization's security and mobility policies. In the event that a user violates this policy, Lookout can block jailbroken and rooted devices from accessing any company apps or data until the device is brought back into compliance. Users can disable the unc0ver jailbreak by rebooting their device.

See Lookout detecting unc0ver here: https://vimeo.com/422853944

Why Lookout

Lookout Mobile Endpoint Security ensures security and compliance on every device, leveraging a large data set fed by over 180 million devices and the analysis of over 100 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.