ProPublica | *Journalism in the Public Interest*

Telecoms, Manufacturers Delaying Critical Patches for Classified Military Smartphones

Telecom carriers and manufacturers are holding back critical software updates putting classified information at risk.

by Jeff Larson, ProPublica
Nov. 9, 2015, 5:30 a.m.

US military personnel take photos of President Barack Obama after his remarks to US Forces Korea and Korean troops in Seoul. (LEE JIN-MAN/AFP/Getty Images)

This story was co-published with the Daily Beast.

You would think the nation's military would move with lightning speed to patch cell phones vulnerable to hackers, particularly after recent disclosures that Chinese hackers harvested the personal information of 21.5 million U.S. government employees and Iran's Revolutionary Guard broke into the Obama Administration's social media accounts.

You would be wrong.

For nearly five months, military officials and officers have continued to use phones that can be attacked by the "Stagefright" bugs, a collection of flaws in the phones' software code that gives attackers access to everything that flows through compromised devices. The bugs can expose those devices to hackers through a simple text message or a visit to the wrong web site.

We asked the various players in the supply chain that winds from phone makers, to Google to cell phone carriers to the Pentagon why the military's devices were still vulnerable to the bugs. Not surprisingly, perhaps, everyone blamed someone other than themselves.

This much is clear. The problem arose because the military is now getting its cell phones from the same carriers and manufacturers that serve civilians. Several of them, including Verizon, AT&T, Sprint and T-Mobile, have been slow to address the Stagefright vulnerabilities in the older model Android phones that are used by nearly 1,000 military officials and officers to discuss classified matters. While the federal government at large has a choice between those carriers, Verizon is the military's carrier of choice within the United States.

Civilian customers simply upgrade their phones when a patch is released, but military users must wait until the Pentagon clears the fix.

In the fast-breaking world of hacking, such delays can be an eternity.

Since 2009, the nation's military has been trying to protect its phone communications with a custom built, encrypted cell phone. The device took five years and $36 million to develop, but by the time it was ready for use, the carriers had upgraded to 4G networks with which it was incompatible. The phone was never widely used in any event; reportedly, it was so difficult to use, many officials left it on the shelf.

To fill the gap, the government struck a deal with Verizon, AT&T and other carriers to use relatively cheap Android phones. The move will save almost $300 million for the federal government over the next few years.

Then, in June, a month before the revelation of the Stagefright bugs, the Pentagon announced it was cancelling its custom-built phone.

The move likely deprived late-night comedians of material about the Pentagon's $4,700 cell phone. But it left the military's non-battlefield communications entirely in the hands of the civilian carriers and cellphone manufacturers which deliver the patches when they decide it's necessary.

Security experts told ProPublica that approach invites disaster.

Zuk Avraham, the chief technology officer of Zimperium, the cyber-security company that discovered the Stagefright bug, told ProPublica that unpatched government phones are wide open to attacks by foreign governments or free-lance hackers. "Devices that do not get upgraded are in great danger — especially government devices," Avraham said.

Military officials insist that the phones are safe to use for classified conversations. If hackers have figured out a way to compromise a device through, say, its video text-messaging, officials simply turn off that feature.

"We are able to shut off different features or capabilities of a different device, but we're not able to discuss the specific tactic used to mitigate it," said Lt. Col. Alana Casanova a spokeswoman for the Defense Information Systems Agency, or DISA, the military's information technology department.

Whenever a new bug comes out, they are stuck waiting for the patches to turn features back on. "The carriers are the ones that push those patches through," she said, "when we're satisfied with them, we flip our switch and we're back in business."

In an email, another spokesperson for DISA would not elaborate on the exact features they've turned off or which patches they've applied. "To do so could assist those without a need to know and potential adversaries who may use the aggregate data to their advantage to undermine the DoD's cybersecurity and, ultimately, national security," the spokesperson wrote.

Avraham said the military's approach poses unnecessary risks. As long as the vulnerable code remains on a device, it can be exploited by hackers clever enough to access it through other means. "Unpatched devices will get hacked," Avraham said. "It is only a matter of time."

Here's how the blame game shook out when we contacted the various participants in the supply chain between phone makers and the Pentagon.

Google, which writes the code for the Android operating system, said it sends out patches every month. The company, which also makes and sells its own cell phones, immediately moved to wall off its devices from Stagefright, but the fix introduced new bugs. Last month, Google automatically upgraded the phones it sells with 15 fixes for the Stagefright bugs.

Verizon did not send out patches for those bugs until late October, almost two months after they were aware of them. "The latest update that's being pushed out now includes the Android security patches for Stagefright," said Verizon spokesman Albert Ayden on Oct. 20.

But according to its website, Verizon only provided patches for the newest phones. That means many of the military's devices, which are older models, remain vulnerable. Verizon did not respond to multiple requests for clarification.

Both AT&T and T-Mobile said that they were waiting for Samsung, the manufacturer of their Android phone, to provide patches. "You need to contact Google and Samsung," said Emily Edmonds, a spokeswoman for AT&T.

A Samsung spokesperson countered that the company had already provided the fix "to all U.S. carriers as part of our monthly Android Security Update." She said Samsung is "working closely with our carrier partners as they roll out the update."

She noted that Samsung phones use a proprietary technology called KNOX that is supposed to protect against hackers. "Samsung mobile solutions for government incorporates many levels of security including Samsung KNOX for enterprise. Government devices with Samsung KNOX for enterprise are protected from Stagefright," she contended.

Avraham, the security expert at Zimperium, disgreed, saying: "KNOX containers definitely help. In this case, containers can be bypassed." He said his company was now working with Samsung's KNOX team to shield users from that vulnerability.

Defense Department officials, for their part, insisted that the phones were secure against hackers, even if the patches were not yet in place.

The military protects its phones through a process known as “defense in depth.” All traffic is funneled through firewalls that are designed to filter out emails and web traffic containing code known to be malicious. Officials said that even when the firewalls weren’t sufficient to prevent exploitation of Stagefright, they can turn off vulnerable features of the phones.

But the world’s hackers have proven remarkably resourceful at figuring out ways to defeat the government’s firewalls. Just this year, the State Department, the White House and the Office of Personnel Management have been reported to have been attacked by Chinese and Russian hackers.

The agency responsible for the military’s cyber-security, DISA, has publicly released manuals instructing military IT officers how to implement workarounds for software bugs that can get through their firewall.

Avraham said the military was adding to the vulnerability of its system by insisting on independently testing each patch after it was approved by Google, Samsung and the carriers.

When asked how important patching software quickly was, Avraham replied “From one to ten? Ten.”