RISK ASSESSMENT / SECURITY & HACKTIVISM

Beware of the text message that crashes iPhones

Newly discovered iOS bug triggers wave of text messages that causes iDevice reboot.

by **Dan Goodin** - May 27, 2015 10:21am PDT

106

Calerusnak

There's yet another iOS bug that causes Apple devices to crash when they receive text messages containing a string of special characters. With further finessing, the same exploit may be able to attack Macs, since OS X is also unable to process the same combination of characters, which are technically known as glyphs.

The menacing combination of ASCII and unicode-based characters looks like this:

effective.

Power

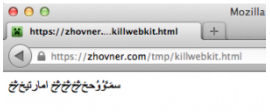
لُلصّبُلُلصّبُررً ◌ّ ◌ّh ◌ّ ◌ّ

ก็

Enlarge

According to people investigating the bug on reddit, the text causes iPhones running various versions of iOS to promptly crash. A flurry of Twitter users, angry that their devices fell victim to text messages, indicates that the bug is causing problems. Apple will almost certainly issue a fix. In the meantime, users can protect themselves against the nuisance text by going to system settings, navigating to Notifications>Messages>Show Previews, and turning it to off.

FURTHER READING



RENDERING BUG CRASHES OS X, IOS APPS WITH STRING OF ARABIC CHARACTERS (UPDATED)

CoreText bug crashes any iOS 6 and OS X programs that use the API.

That change will prevent attacks that are currently circulating online, but it may not stop miscreants from finding new ways to crash people's iDevices. According to the reddit thread, messages sent over WhatsApp may also trigger the crash. And depending on the way individual apps parse Unicode glyphs, other programs may do the same thing. The bug can also trip up OS X, although the attack requires a target to concatenate or paste a malicious file into the Mac terminal, according to a researcher who goes by the Twitter handle Hacker Fantastic.

Hacker Fantastic has tweeted a variety of other interesting technical details. The bug, he reported, resides in a part of the operating system that processes Unicode glyphs and causes a string to be written to a particular memory location. The bug is tied to the way banner notifications process Unicode, reddit reader sickestdancer98 reported. The banner is unable to display the text and eventually crashes the entire OS.

FURTHER READING

IOS BUG SENDS IPHONES INTO ENDLESS CRASH CYCLE WHEN EXPOSED TO ROGUE WI-FI

SSL cert parsing error allows attackers to create "No iOS Zone," researchers say.

While the bug is rightfully regarded primarily as a nuisance, denial-of-service vulnerabilities can often be the result of serious flaws that, with more work, can be exploited to perform code-execution attacks. And even when more malicious exploits aren't possible, DoS holes can sometimes present opportunities for extortionists or people looking to disrupt large events—for instance people at a conference. Expect Apple to release a patch in the coming week or so.

PROMOTED COMMENTS

d0x | Wise, Aged Ars Veteran jump to post

> Thoughtful wrote:
> I'm interested in *how* a text string can so badly break things. Time to follow the article's links

America online used to have the same issues but lots more of them. The best was [font size = 99999999...9999]

It would cause AOL to instantly crash. Also opening and closing html tags with a letter in between each set would cause AOL to show a single letter at a time. The more letters the longer it took to display them and while this was happening the person you sent the IM to or the chatroom would be frozen. This got real bad when AIM was released and people would use bots to scrape names from public chats and mass "punt" them all offline.

112 posts | registered Sep 7, 2011

Rosyna | Ars Tribunus Militum jump to post

> fuzzyfuzzyfungus wrote:
> show nested quotes

My question isn't why the rendering bugs exist(as you say, Unicode is a spec that attempts to handle enough symbols to handle every *natural language* of any relevance, along with a bunch of other stuff, so it's one mean bundle of pain); but why it is in the position to crash the OS.

I would have assumed that(for security reasons, if nothing else) the dangerous business of doing complex things to input from untrusted sources and displaying the results to the user would be kept

TAKE ME THERE

Google Maps allows turn-by-turn navigation—offline

UT SIS FELIX TIBI PECUNIA OPUS

The Dealmaster wants to offer you a moment of Zen(book)

UN says encryption "necessary for the exercise of the right to freedom"

> well away from the kernel and other important things, as isolated as possible in its own little process that can, if things go wrong, eat its own brain and die without the rest of the system being affected.
>
> I would have been utterly unsurprised by a rendering bug that trashed the heck out of that particular message bubble, or took down the entire app that handles texts and iMessage traffic; but the OS, why?

The bug/crash issue exists in the process that displays notifications, which is SpringBoard (one of the reasons disabling notifications fixes it).

The bug seems to cause the process to go into a recursive, infinite loop, using up an insane amount of resources until there are no more resources left. There seem to be two outcomes to this starvation:

1. The process (SpringBoard) crashes. This causes everything to flash as springboard gets relaunched. SpringBoard is an extremely important process as it handles multiple things. It's possible its death can result in a reboot since it's never supposed to die.
2. The iPhone, starving of resources, does panic(), forcing a reboot.

Since I can't actually get it to crash my iPhone 6 Plus (it appears to depend on where the text is truncated), I am guessing a little on the processes involved but Messages itself is not the process that is dying.

But since the crash is in SpringBoard, it should work for any notification, including those from other apps (and shared Calendars!)

Maybe even AirDrop?

2597 posts | registered Sep 4, 2005

1386 | **Smack-Fu Master, in training** **jump to post**

> iolinux333 wrote:
> The iMessage server seems to be blocking this particular string from getting through now. Fun over.

I thought imessages were supposed to be end to end encrypted. If that's true, how could they block it? Regardless, I was able to send this to myself with no ill effects ios 8.3, iphone 5

29 posts | registered Sep 26, 2012

READER COMMENTS 106

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE