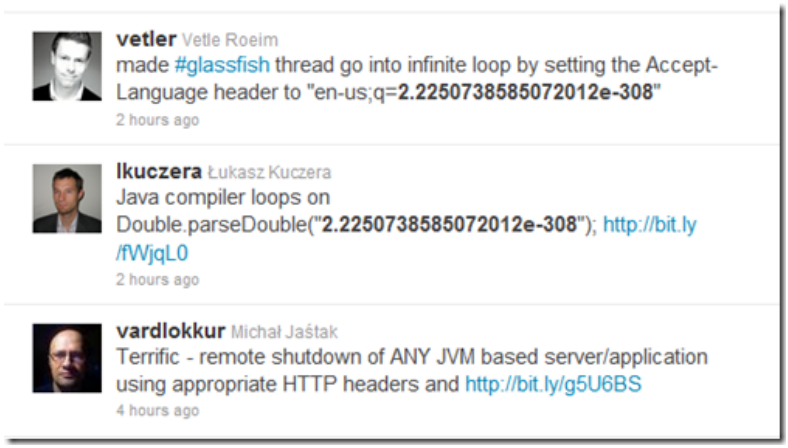
Mitigate Java Vulnerability with iRules

Jason Rahm, 2011-03-02

I got a request yesterday morning to asking if there was a way to drop HTTP requests if a certain number was referenced in the Accept-Language header. The user referenced this post on Exploring Binary. The number, 2.2250738585072012e-308, causes the Java runtime and compiler to go into an infinite loop when converting it to double-precision binary floating-point. Not good. Twitter is ablaze on the issue, and there is a good discussion thread on Hacker News as well. So how do you stop it? At first, this appeared to be a no-brainer, just copy that string and drop if found in that header, right? Well, there's a catch. A few actually. This number can be represented in many ways:



- Decimal point placement => 0.00022250738585072012e-304
- Leading Zeroes => 00000000002.2250738585072012e-308
- Trailing Zeroes => 2.22507385850720120000e-308
- Leading Zeroes in the Exponent => 2.2250738585072012e-00308
- Superfluous Digits past digit 17 => 2.22507385850720129978000001e-308

String match seemed the perfect fit for this as I need a few wildcards to sort this out. I started in the Tcl shell just to make sure all the use cases matched:

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113