LUNATECH
RESEARCH

DoS vulnerability in Play <= 1.2.4

2012-01-06 – Erik Bakker - @eamelink - lunatech.com

The Vulnerability

#Disclosed by n.runs AG, a German security company on December 28, 2011

#Affects PHP, Oracle, Microsoft, Python, Ruby, Google, Java, Apache Tomcat, Apache Geronimo, Jetty, Glassfish, ASP.NET, Python, Plone, V8

The Vulnerability

- Disclosed by n.runs AG, a German security company on December 28, 2011
- Affects PHP, Oracle, Microsoft, Python, Ruby, Google, Java, Apache Tomcat, Apache Geronimo, Jetty, Glassfish, ASP.NET, Python, Plone, V8
- ... and Play 1.2.4

The theory

#Web frameworks put POST parameters in a Hashmap

#Hashmap inserts take constant time

#But for n keys with the same hash, insert time grows with $O(n^2)$

Hash Collisions in Java

#Finding strings with the same hashCode in Java is easy. "Aa" and "BB" have the same hashcode...

#And so do "AaAa", "AaBB", "BBAa" and "BBBB"

#Easy to generate infinitely many strings with the same hashcode!

The Solution

#Use a better datastructure

#Limit the number of POST parameters

LUNATECH
RESEARCH

DoS vulnerability in Play <= 1.2.4

2012-01-06 – Erik Bakker - @eamelink - lunatech.com