

QGIS Application - Bug report #5413

Virus in grass-6.4.2 package, QGIS 1.7.4

2012-04-19 02:46 AM - Lars Cremer

Status: Rejected	
Priority: High	
Assignee:	
Category:	
Affected QGIS version: 1.7.4	Regression?: No
Operating System:	Easy fix?: No
Pull Request or Patch supplied:	Resolution: invalid
Crashes QGIS or corrupts data:	Copied to github as #: 15078

Description

Hello,

my proxyserver detect a virus in a package.

This is the error from the server:

IWSS Security Event

InterScan Web Security detected malicious code in your web traffic:

Item: <http://www.qgis.org/downloads/QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe>

Action: deleted

Infection detail:

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/bin/d.colors.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/bin/r.sim.sediment.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/bin/r.sim.water.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/bin/v.surf.rst.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/driver/db/ogr.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/driver/db/pg.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

-- File: \$_OUTDIR/apps/grass/grass-6.4.2/driver/db/sqlite.exe, Enclosure: QGIS-OSGeo4W-1.7.4-d211b16-Setup.exe, malicious code name: PAK_Generic.001

The uncleanable file is deleted.

Kind regards

Lars

Related issues:

Duplicated by QGIS Application - Bug report # 6082: QGis download Malicious V...

Closed

2012-07-23

History

#1 - 2012-04-19 03:12 AM - Jürgen Fischer

- *Resolution set to invalid*
- *Status changed from Open to Rejected*

Most probably a false positive. See [Trojan in OSgeo Windows download package](#)

<http://www.garyshood.com/virus/> also reports the 1.7.4 as clean (i.e. Clamav, F-PROT, Antivir, BitDefender and AVG)