Bug 1896739 (CVE-2020-25708) - CVE-2020-25708 libvncserver: libvncserver/rfbserver.c has a divide by zero which could result in DoS

Keywords:	Security ×
Status:	CLOSED ERRATA
Alias:	CVE-2020-25708
Product:	Security Response
Component:	vulnerability
Version:	unspecified
Hardware:	All
OS:	Linux
Priority:	medium
Severity:	medium
Target Milestone:	---
Assignee:	Red Hat Product Security
QA Contact:	
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	~~1896740~~ 1898077 1898078
Blocks:	1896743
TreeView+	depends on / blocked

Reported:	2020-11-11 12:39 UTC by Michael Kaplan
Modified:	2021-05-18 15:16 UTC (History)
CC List:	5 users (show)
Fixed In Version:	libvncserver 0.9.13
Doc Type:	If docs needed, set a value
Doc Text:	A divide by zero flaw was found in libvncserver. This flaw allows a malicious client to send a specially crafted message that, when processed by the VNC server, leads to a floating-point exception, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
Clone Of:	
Environment:	
Last Closed:	2021-05-18 14:36:07 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Michael Kaplan 2020-11-11 12:39:52 UTC Description

An issue was discovered in libvncserver-0.9.12. There is a divide by zero in rfbSendRectEncodingRaw function in libvncserver/rfbserver.c.
Attackers can launch a denial of service attack by sending a special message to the VNC server.

Upstream issue:
https://github.com/LibVNC/libvncserver/issues/409

Upstream commit:
https://github.com/LibVNC/libvncserver/commit/673c07a75ed844d74676f3ccdcfdc706a7052dba

Michael Kaplan 2020-11-11 12:39:58 UTC Comment 1

Acknowledgments:

Name: Kailong Zhu, Hui Huang, Lu Yu

Michael Kaplan 2020-11-11 12:40:02 UTC Comment 2

External References:

https://github.com/LibVNC/libvncserver/issues/409
https://github.com/LibVNC/libvncserver/commit/673c07a75ed844d74676f3ccdcfdc706a7052dba

Michael Kaplan 2020-11-11 12:40:40 UTC Comment 3

Created libvncserver tracking bugs for this issue:

Affects: epel-7 [~~bug 1896740~~]

DRC 2021-02-23 21:49:30 UTC Comment 7

NOTE: at least one commercial firewall has flagged TurboVNC connections as vulnerable to this CVE, but to the best of my knowledge and testing, LibVNCServer is the only TightVNC-compatible code base that is (was) vulnerable. I was unable to reproduce the vulnerability with TightVNC 1.3.x, TigerVNC, or TurboVNC. Refer to https://github.com/TurboVNC/turbovnc/pull/273#issuecomment-784498698.

Product Security DevOps Team 2021-05-18 14:36:07 UTC Comment 9

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-25708

errata-xmlrpc 2021-05-18 15:16:21 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2021:1811 https://access.redhat.com/errata/RHSA-2021:1811

Note
You need to log in before you can comment on or make changes to this bug.