Bugs versus vulnerabilities?

Asked 15 years, 11 months ago   Modified 15 years, 11 months ago

Viewed 12k times

▲

16

▼

What, if any, is the difference between a software bug and a software vulnerability?
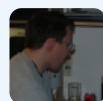
security

Share

Improve this question

Follow

9 Answers

Sorted by: Highest score (default) ⇕

▲

34

▼

✓

A bug is when a system isn't behaving as it's designed to behave.

A vulnerability is a way of abusing the system (most commonly in a security-related way) - whether that's due to a design fault or an implementation fault. In other words, something can have a vulnerability due to a defective design, even if the implementation of that design is perfect.

Share   Improve this answer

Although one could say that the design has a bug. – Robert Gamble Dec 31, 2008 at 13:15

+1: A bug may or may not introduce a vulnerability. A vulnerability is a problem, and could be classified under the heading of "bug". – S.Lott Dec 31, 2008 at 13:15

i agree with robert's comment - the system may be behaving as designed, and still have a bug because the design does not meet the requirements. – frankodwyer Dec 31, 2008 at 13:37

1 @frankodywer/Robert: I *tend* to regard "bug" as an implementation word, rather than just any kind of defect. You could certainly say that the design was defective - or perhaps even the requirements. – Jon Skeet Dec 31, 2008 at 13:58

@jon - that makes sense. and if you define bug that way, vulnerability is not a subset of bug. – frankodwyer Dec 31, 2008 at 14:12

▲

11

▼

🔖

🕐

Vulnerability is a subset of **bug**.

A bug is *any* defect in a product.

A vulnerability is bug that manifests as an opportunity for malicious use of the product. Vulnerabilities generally are not that clearly evident, but require ingenuity to be exploited.

Share   Improve this answer   answered Dec 31, 2008 at 13:15

Follow

To the drive-by downvoter: If you are going to downvote an answer with nothing clearly wrong with it the least you can do is explain why. – Robert Gamble Dec 31, 2008 at 13:32

I didn't downvote this however I think a minor issue in this answer is that a vulnerability is more than an opportunity for malicious use of the product. for example if your web infrastructure is vulnerable to DDOS (and most are), your system is too. But I wouldn't call that a 'malicious use'. – frankodwyer Dec 31, 2008 at 13:41

But the answer doesn't say a vulnerability is just an opportunity for malicious use, it says a vulnerability is a *bug* with the opportunity for malicious use. – Robert Gamble Dec 31, 2008 at 13:47

Well, regardless of the constitution of the code, if there is no malicious intent out there, there is no vulnerability in my program. – G S Dec 31, 2008 at 13:52

@Fredrick - There is always malicious intent present if your code connects to the Internet. :) – romandas Dec 31, 2008 at 13:57
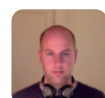

▲

4

▼

The two can sometimes overlap, but I'd say a "bug" is a mistake, while a "vulnerability" is, like the name suggests, a weakness.

Share Improve this answer

Follow

🔖

answered Dec 31, 2008 at 13:10
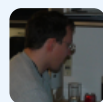
Bart Kiers
170k ● 37 ● 305 ● 295

2

From a programming perspective, I believe there is no difference between a bug and a vulnerability. They are both mistakes in the software.

However, from a security perspective, a vulnerability is a class of bugs that can be manipulated in some fashion by a malicious person.

Share Improve this answer

Follow

answered Dec 31, 2008 at 13:09

romandas
4,206 ● 7 ● 30 ● 34

---

although I guess that a vulnerability does not have to be a bug, it could be a concious decision not to handle a case - for example based on an analysis of the cost/impact/likelyhood of the vulnerability – Yossi Dahan Dec 31, 2008 at 13:11

They don't have to be the same. As Yossi said, not all vulnerabilities are bugs. And not all bugs are vulnerabilities. A bug might just be an annoyance, or broken functionality, without being exploitable, and so it's not really a vulnerability. It's just broken :p – Stack Overflow is garbage Dec 31, 2008 at 13:16

@Yossi - Interesting idea; so, one could intentionally design vulnerable software, but the vulnerability would not be a bug in that case? – romandas Dec 31, 2008 at 13:23

---

vulnerabilities aren't always mistakes in your software, however. for example if the platform you depend on is vulnerable, you have a problem too. – frankodwyer Dec 31, 2008 at 13:34

@frankodwyer - That seems outside the scope of my question, which was comparing a software bug to a software vulnerability. If the platform's software is vulnerable, there is a software vulnerability. If it's something else (hardware, physical, etc), it's out of scope. – romandas Dec 31, 2008 at 13:46

A bug is a failure of your system to meet requirements.

2

Vulnerability is a subset of bug - it is when your system can be forced into a failure mode that does not meet requirements, usually by (ab)using your system (or something your system relies on) in an unexpected way.

Usually a vulnerability may result in failure to meet a requirement in one or more of these areas:

- confidentiality

- integrity

- availability

or you can combine the last two:

- confidentiality

- reliability (= integrity + availability)

Share Improve this answer

Follow

edited Dec 31, 2008 at 13:31

answered Dec 31, 2008 at 13:19

If you use Bugzilla, anything you need to do something with is a bug ;)

1

Share   Improve this answer

Follow

answered Dec 31, 2008 at 16:44

community wiki
Ola Eldøy

That is a good point (misnomers in software).
– Peter Mortensen Jan 19, 2023 at 16:31

In my eyes vulnerabilities are a subset of bugs that enable someone to perform a malicious or harmful operation with your software.

0

Bugs are just code that does not work properly (how you define properly is subject to opinion).

Share   Improve this answer

Follow

answered Dec 31, 2008 at 13:12

Garry Shutler
32.7k ● 13 ● 89 ● 120

Wikipedia:

0

> In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system

For example, home computers are vulnerable to physical threats like flood and hand grenades, but they are not considered a "bug". In enterprise environment, these threats are treated with more seriousness if the risk of system shutting down is great enough, maybe for air traffic support or nuclear reactor management.

Business continuity planning/disaster recovery and high availability usually deals with physical threats and failures by redundant hardware and distributing servers to remote locations.

Classification of software defect (or "bug") can be subjective, since it depends on the intent of the software design and requirements. A feature for a given set of audience may be interpreted as a vulnerability to the other if abused. For example, stackoverflow.com now discloses self-closed questions to those with 10k reps. Some may say it is a vulnerability since it violates common expectation of ordinary users (Like I said, it's a subjective call).

Share   Improve this answer

Follow

edited May 23, 2017 at 12:30

Community Bot
1 ● 1

answered Dec 31, 2008 at 14:04

The question is specific to software vulnerabilities. An earthquake isn't a "bug". :) – romandas Dec 31, 2008 at 14:15

0

A bug is the failure of software to meet requirements. I would consider these to be the ideal requirements, so it would make sense to say that there's a bug in the requirements analysis, although that's more debatable.

A vulnerability is a feature, intended or otherwise, that can be exploited maliciously. It is not necessarily a bug, provided that it was deliberate.

To change subjects, it is a vulnerability that my home wireless has a guessable WPA password, but that was a conscious choice, to facilitate use by my guests. That's an example of requirements leading to a vulnerability. If I'd entered a weak password because I didn't know better, that would have been a bug as well as a vulnerability.

Share Improve this answer

Follow

answered Dec 31, 2008 at 15:35

David Thornley
57k ● 9 ● 95 ● 158