Zero-Day

Return to Glossary

A **Zero-Day** (also known as **0-day**) is a computer-software vulnerability unknown to those who should be interested in its mitigation (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers, or a network.[1] An exploit directed at a zero-day is called a zero-day exploit, or zero-day attack.

The term “zero-day” originally referred to the number of days since a new piece of software was released to the public, so “zero-day software” was obtained by hacking into a developer's computer before release. Eventually, the term was applied to the vulnerabilities that allowed this hacking, and to the number of days that the vendor has had to fix them. Once the vendor learns of the vulnerability, they will usually create patches or advise workarounds to mitigate it.

Source: https://en.wikipedia.org/wiki/Zero-day_(computing)