A vulnerability in software that the developer or vendor is yet unaware of and therefore hasn't mitigated, is called a zero-day.

The name zero-days is derived from the fact the exploit is not known by the developers and therefore they had no days to fix it.

Criminals may exploit these using malware in what is known as zero-day attacks, or a zero-day exploit when they use the vulnerability to access or otherwise compromise the network.

Zero-day attacks are a dangerous cybersecurity threat, as while the vulnerability is not widely known, has no code fix through a patch, and not mitigations criminals can misuse these until the vulnerability becomes known.

Security patches or mitigations may take some time to be produced, meanwhile the criminals continue to exploit the software.

A well-publicised zero-day that was exploited to large effect on critical infrastructure, was the Stuxnet malware that exploited multiple vulnerabilities that were present at the time in the Microsoft Operating System.