# Cyber vulnerabilities, maintenance releases, CVE's - what's it all about?

Gallagher has a goal of being the most cyber secure physical security manufacturer and actively seeks to identify possible vulnerabilities in our platforms. A cyber security vulnerability is a weakness that would allow a cyber attacker to make a computer system misbehave. At one extreme, a vulnerability could allow an attacker to open a secure door, but vulnerabilities can also allow an attacker to retrieve information or disrupt the normal operation of a system.

A CVE (Common Vulnerability and Exposure) is a report that describes a vulnerability in a software/computer system. The CVE website hosts the list of all CVE's and allows the list to be searched by number or keyword, for example "Gallagher". We're proud to be one of only approximately 220 companies in the world who are an authorized CVE Numbering Authority and you can read more about our journey to becoming authorized with CVE here.

Gallagher lists all of our CVE's and vulnerabilities on our website where we provide a description, vulnerable versions of our system, and possible mitigations. There is additional information about the priority and scoring criteria that an experienced IT professional will understand.

Vulnerabilities are identified by our team and there is a formal triage and prioritization process that will have our critical and high vulnerabilities fixed as quickly as possible. We also have a Responsible Disclosure Policy, which allows security researchers to work with us and disclose vulnerabilities in a safe and well-defined manner, so that we can minimize harm to our users. Where we have confidence that a vulnerability is not likely to be actively exploited on customer sites, we will fix the issue first, followed by a process to release version updates and inform Gallagher teams, you - our Channel Partners, and then publish to the CVE website.

When fixing an issue, a critical or high vulnerability will be fixed in the latest software release plus the three prior releases. Lower priority vulnerabilities may only be fixed in the most recent couple of software releases. Our maintenance releases (MR) of a software version will have a version number such as “v8.40.1888(MR3)” where the “8.40” is the version of the software feature set, the “1888” is an incremental “build” which our teams use to uniquely identify the software down to individual bug and vulnerability fixes. The “(MR3)” is there to give an easy descriptor for our Gallagher team and your team members, to identify a unique version.

Two weeks prior to publishing a vulnerability on our own website and the CVE website , we will send out a security advisory to you, our Channel Partners. This will indicate the highest severity vulnerability in the release or maintenance releases. Our technical teams will also have received this information. At this point we prefer not to publish the full text of the CVE. This is to prevent an attacker from using that information to identify where to look in the product and exploit the vulnerability prior to the update being released, or before there is an opportunity for a customer to upgrade their system.

We recommend that all our customers upgrade to the latest version or MR for their current version to ensure their system is as secure as it can possibly be. With this in mind, we understand that the process can be costly for some customers in some situations. Where possible, we will ease the upgrade process to affect as few of the components of the system (server, workstation, controllers) as possible in the fix process so that the impact of an upgrade is minimized.