Understanding Automox Severity Data

Where does the vulnerability severity score come from and how is it calculated? What are the effects on my patching?

Learn about the following topics here:

- Automox severity scoring
- When is severity information updated?
- Why am I patching more?
- What does a severity of High indicate and should I be concerned?
- What does a score of None indicate?

Severity information used by Automox originates from OS and app providers. An independent group of security researchers calculates the CVSS severity score. How this is calculated is described in the National Vulnerability Database.

Automox severity scoring

The severity of CVEs are based on CVSS scores. These scores have different mappings to severity classifications. The following mapping table shows how Automox defines the previous version 2 and the new version 3 severity ratings of a package:

<table>
<thead>
<tr>
<th>Automox CVSSv2</th>
<th>Automox CVSSv3</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>(0.0)</td>
</tr>
<tr>
<td>Low</td>
<td>(0.0–3.9)</td>
</tr>
<tr>
<td>Medium</td>
<td>(4.0–6.9)</td>
</tr>
<tr>
<td>Critical</td>
<td>(7.0–10)</td>
</tr>
<tr>
<td>Other</td>
<td>Not scored</td>
</tr>
</tbody>
</table>

In the event that there are multiple CVEs, with a mixture of scores, the highest possible CVSS score will determine the severity.

Note: If a CVE is not scored or Automox has insufficient information, it will be shown as Unknown.

When is severity information updated?

When a device scan happens (either automatically or manually), the severity data presented in the console will be accurate to within the last 1-hour time span. Upon your group scan interval, this data will be presented.
Note: New severity information does not cause the device to patch. Your patching schedule determines when the patch is applied.

Why am I patching more?

The introduction of the Automox CVSSv3 severity scoring model can mean increased patching.

- Policy scopes might change with the introduction of the categories High and None.
- Depending on your configuration, the pending (or scheduled patch) counts can go up or down as a result.
- With better severity information, legacy patches can suddenly appear, although they were not previously marked for patching.

What does a severity of High indicate and should I be concerned?

Yes, you should be concerned. A High patch score usually indicates severe exploits that might require additional complexity for a hacker to use. This refers to someone who gains physical access to the machine or relies on another unpatched exploit to gain access. These are serious and would have been considered Critical in the previous severity scoring. Unless you have a reason to not include High patches, you should patch them.

What does a score of None indicate?

A severity level of None is equal to a score of 0.0. This indicates that there are no known vulnerabilities associated with the patch.