Vulnerability Remediation Timelines / Service Level Agreement

Vulnerability Type	Critical (9.0-10.0)	High (7.0-8.9)	Medium (4.0-6.9)	Low (0.0-3.9)
Rapid Response	14 days	n/a	n/a	n/a
External-Facing	30 days	60 days	90 days	547 days
Internal	90 days	180 days	365 days	547 days

- The days listed in each **SLA Timeline** is the expected timeframe to remediate or otherwise address vulnerabilities. This clock for each will **start on the date that we identify it in our environment**. If they're to be addressed through a formal risk exception approval process, because this is still in progress of being built, our team will simply begin collecting requests for review at a later date.
- Vulnerabilities are flagged as **Rapid Response** when they have an elevated risk score, are widely reported with publicly-available exploits, and UR/URMC is believed to have on externally-facing platforms.
- **External-Facing** vulnerabilities are those identified on machines that have services accessible via the public Internet, or are otherwise reachable from outside UR/URMC networks.
- The calculated **Risk Score** next to each severity level (Critical, High, Medium, Low) is the assessed rating of a vulnerability based on the ease and impact of exploit, threat intelligence, exploit maturity, and other factors.