

The following matrix is a guide for what is typically escalated for patching at [org], but should be used

as a guideline only - analysts should use their best judgement in interpretation of threat intelligence

sources to make a determination of expedited patching or PatchNow is required and this

determination should be made in conjunction with InfoSec leadership

1. Gather appropriate details about the vulnerability or exploit:

a. What is the CVE rating of the vulnerability?

b. What is the scope of the vulnerability? How many assets are [org] are likely vulnerable?

How many of them are internet-exposed?

c. Is any authentication or other requirements for successful execution?

d. What is the level of effort? Is this a type of vulnerability that has been commonly exploited

before?

e. Is there a threat actor group that has been identified? Does that threat actor group have

'common targets' which may include lines of business or functions that [org] participates

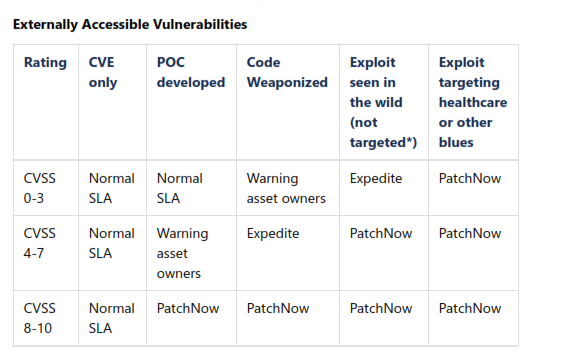
in?

f. Is there any discussion on intelligence networks regarding recommendations, urgency or

likelihood of an exploit in the wild?

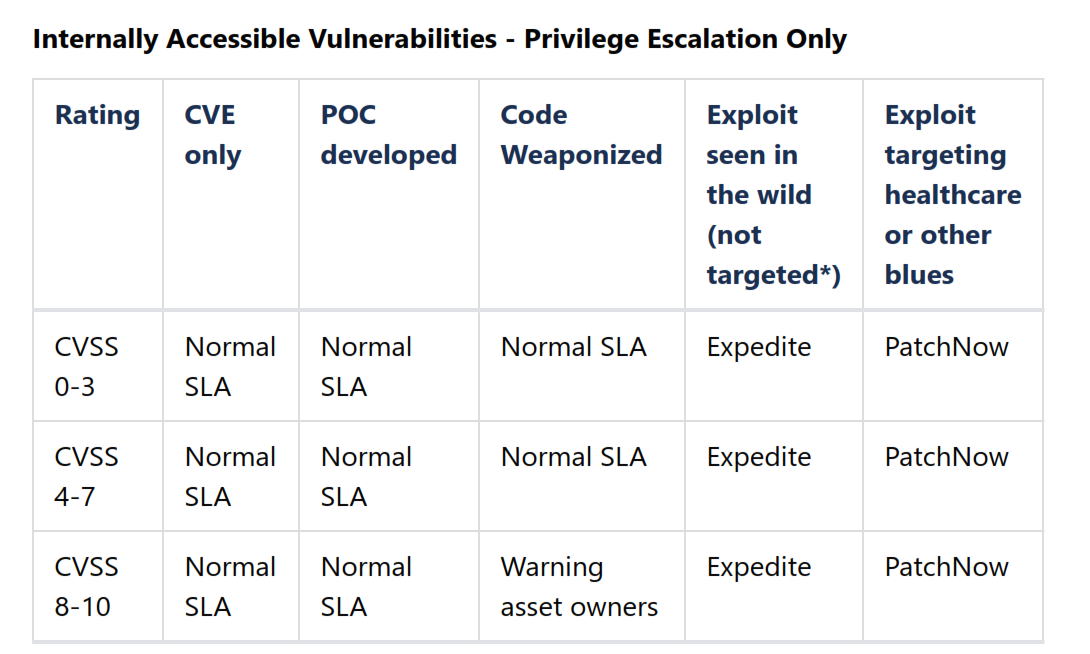
Given this information does it appear that there will be an exploit available before the next

patching cycle will occur?



**Internally Accessible Vulnerabilities**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rating** | **CVE Only** | **POC Developed** | **Code Weaponized** | **Exploit seen in the wild (not targeted)** | **Exploit targeting healthcare or other Blues** |
| 0-3 | Normal SLA | Normal SLA | Warning / heads up issues to patching teams | Expedite | Patch Now |
| 4-7 | Normal SLA | Normal SLA | Warning / heads up issues to patching teams | Expedite | Patch Now |
| 8-10 | Normal SLA | Normal SLA | Expedite | Expedite | Patch Now |



**\*Not targeted = while the exploit is seen in the wild, it appears to be targeted to other industries or**

**lines of business not applicable to [org]. We're less likely to be a target of the active campaign**

**Request consideration for escalation:**

**1. Compose an email to the security team members and copy the CISO**

**Include any relevant details that you may share based on TLP about why you believe this**

**should be an Expedited Patch Request or PatchNow. Include items A-F from above in a**

**summarized form.**

**2. Team agrees request should be made, appropriate team identified for making an expedited patch**

**request (server operations, etc)**

**3. Compose communications according to template below**

**4. If there is a Nessus plugin available for a critical or high vulnerability, remedy ticket will be**

**automatically created. If there is no plugin available, create a ticket in Remedy as a critical incident**

**and assign to the appropriate team, copying the details of the communications**

**5. Go into the "Patch Now" teams workspace and paste the communications, make sure to '@' specific staff (see Ticketing Matrix ) and ask if they need a email sent to them as well to complete the request.**

**6. Record on all details in the Jira ticket. Make sure to add the tag "PatchNow" if activated; which**

**teams are working on the patch now, and an ETA for completed patching. Keep the ticket open**

**and assigned to yourself until you can confirm via Tenable or via emails that the vulnerability as**

**been remediated.**

**7. If the analysis of an active exploit identifies a Threat Actor group or a Attack Technique relevant to**

**[org], consider creating a Jira ticket for a Purple Team assessment.**

**Comms template:**

**Subject:**

**Urgent Patching Request / High Priority Patching Request / Critical Priority Patching Request**

**Email body:**

**This is a request for expedited patching schedule based on information about (CVE details and link here) affecting (describe population. eg. Windows 2008/2008R2) systems. Based on (what information that can be released based on TLP. if unable to provide specific information use the language: due to the critical severity of the vulnerability and the impact of successful execution we believe there is a high likelihood of near-term exploitation by threat actors.)**

**Urgent: Please patch all in scope systems, following normal staging process for patch deployment starting as soon as feasible for the business.**

**High Priority: Please patch all in scope systems, following normal staging process for patch deployment starting IMMEDIATELY**

**Critical: Please patch all in scope systems IMMEDIATELY, forgoing normal staging process for the sake of expedited risk reduction and response to this vulnerability.**

**Note that details on this remediation indicate a reboot is/is not required.**

**Additional compensating controls the Interactive Threat Defense (ITD) team would like where feasible for the business or can recommend:**