HackaTUM

Siemens The Incident Game

Critical Vulnerability

CVE-1900-8033

Remote Unauthenticated Code Execution Vulnerability in Docker

Impact

Data Breaches - Service Disruption - Unauthorized Access to Sensitive data

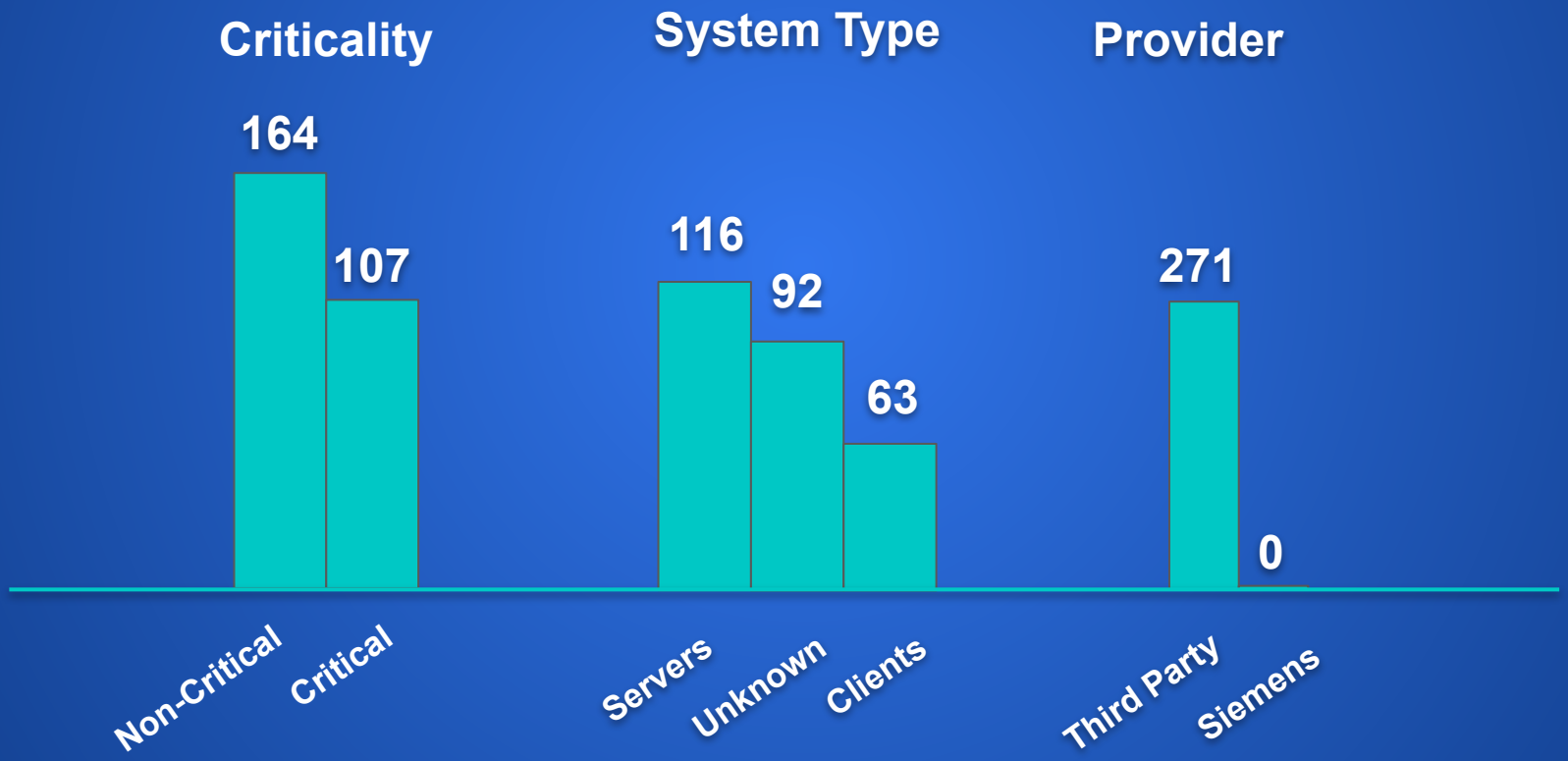
CVSS Score

9.8 - Critical

Solution

None available yet

Overview - # Affected Systems: 271



Approach

Identification

Classification

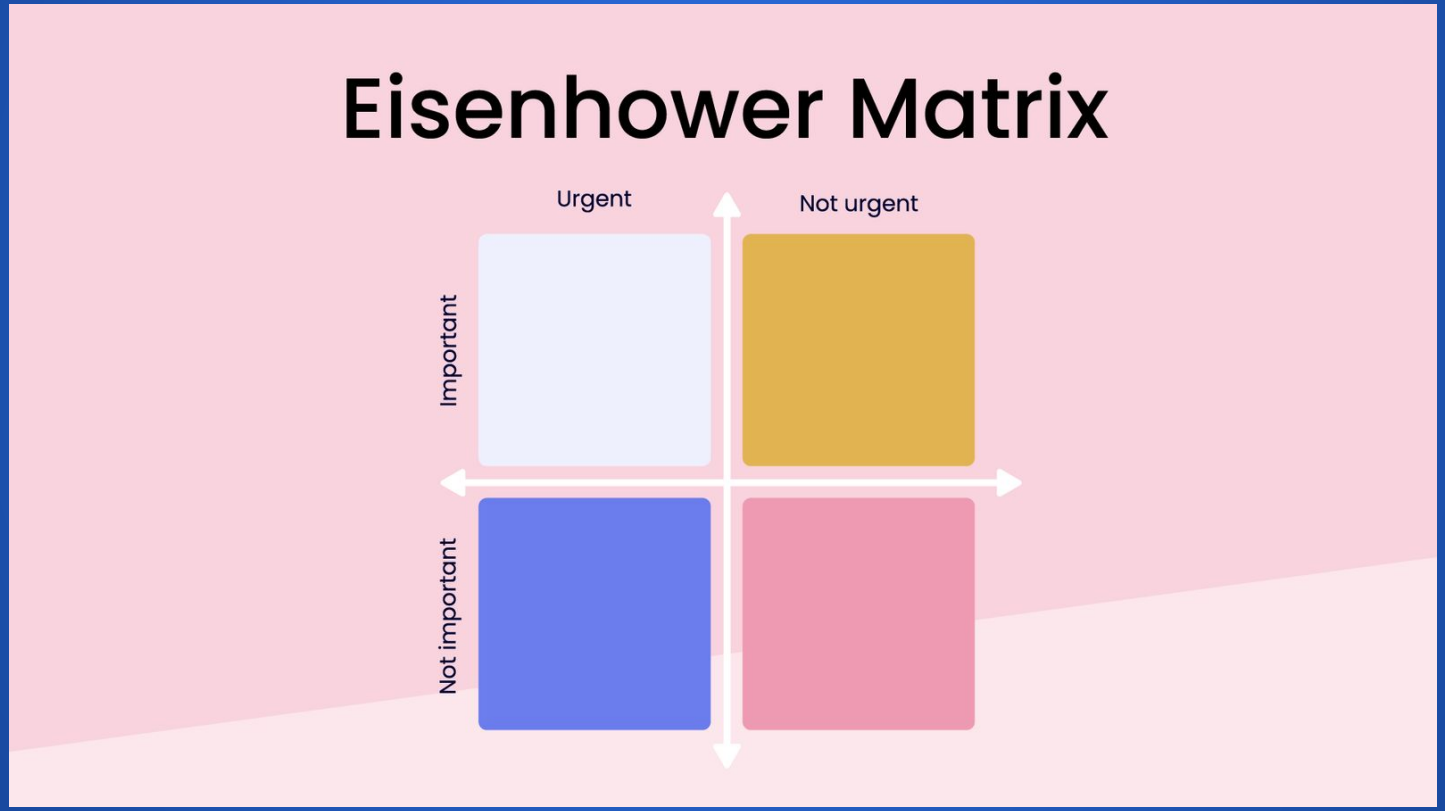
Mitigation

Approach (Identification)

Detection of vulnerable systems based on 2 criteria:

- Is Docker installed on the system?
- Is the installed version vulnerable?

Approach (Classification)



Approach (Classification)

- Prioritize the the mitigation based on the calculated risk
- The risk Formula we used:

```
risk_sum =  (base_cvss_score/10) + (epss_score) + (criticality_score) + (system_type_score/3) + \
            (edr_score) + (provider_score) + (state_score) + (role_score)
# Return a normalized value between 0 and 1
return risk_sum / 8
```

Approach (Mitigation)

- No official fix available currently for CVE-1900-8033
- Install EDR
- Limit network exposure of affected systems
- Update IDS/IPS databases (IoC)