VA Needs to Address Identified Vulnerabilities

What GAO Found

While the Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, it has not fully addressed these weaknesses. For example, VA took actions to contain and eradicate a significant incident detected in 2012 involving a network intrusion, but these actions were not fully effective:

- The department’s Network and Security Operations Center (NSOC) analyzed the incident and documented actions taken in response. However, VA could not produce a report of its forensic analysis of the incident or the digital evidence collected during this analysis to show that the response had been effective. VA’s procedures do not require all evidence related to security incidents to be kept for at least 3 years, as called for by federal guidance. As a result, VA cannot demonstrate the effectiveness of its incident response and may be hindered in assisting in related law enforcement activities.
- VA has not addressed an underlying vulnerability that allowed the incident to occur. Specifically, the department has taken some steps to limit access to the affected system, but, at the time of GAO’s review, VA had not fully implemented a solution for correcting the associated weakness. Without fully addressing the weakness or applying compensating controls, increased risk exists that such an incident could recur.
- Further, VA’s policies did not provide the NSOC with sufficient authority to access activity logs on VA’s networks, hindering its ability to determine if incidents have been adequately addressed. In an April 2014 report, GAO recommended that VA revise its incident response policies to ensure the incident response team had adequate authority, and VA concurred.

Further, VA’s actions to address vulnerabilities identified in two key web applications were insufficient. The NSOC identified vulnerabilities in these applications through testing conducted as part of the system authorization process, but VA did not develop plans of action and milestones for correcting the vulnerabilities, resulting in less assurance that these weaknesses would be corrected in a timely and effective manner.

Finally, vulnerabilities identified in VA’s workstations (e.g., laptop computers) had not been corrected. Specifically, 10 critical software patches had been available for periods ranging from 4 to 31 months without being applied to workstations, even though VA policy requires critical patches to be applied within 30 days. There were multiple occurrences of each missing patch, ranging from about 9,200 to 286,700, and each patch was to address an average of 30 security vulnerabilities. VA decided not to apply 3 of the 10 patches until it could test their impact on its applications; however, it did not document compensating controls or plans to migrate to systems that support up-to-date security features. While the department has established an organization to improve its vulnerability remediation, it has yet to identify specific actions and milestones for carrying out related responsibilities. Until VA fully addresses previously identified security weaknesses, its information is at heightened risk of unauthorized access, modification, and disclosure and its systems at risk of disruption.