The increase in reported information systems vulnerabilities has been staggering, especially in the past 3 years (see chart). Automated attacks are successfully exploiting such software vulnerabilities, as increasingly sophisticated hacking tools become more readily available and easier to use. The response to two recent critical vulnerabilities in Microsoft Corporation and Cisco Systems, Inc., products illustrates the collaborative efforts between federal entities and the information security community to combat potential attacks.

Patch management is one means of dealing with these increasing vulnerabilities to cybersecurity. Critical elements to the patch management process include management support, standardized policies, dedicated resources, risk assessment, and testing. In addition to working with software vendors and security research groups to develop patches or temporary solutions, the federal government has taken a number of other steps to address software vulnerabilities. For example, offered without charge to federal agencies, the federal patch notification service provides subscribers with information on trusted, authenticated patches available for their technologies. At present, the government is considering broadening the scope of these services and capabilities, along with the number of users. Other specific tools also exist that can assist in performing patch management.

In addition to implementing effective patch management practices, several additional steps can be taken when addressing software vulnerabilities. Such steps include stronger software engineering practices and continuing research and development into new approaches toward computer security.