CISA Urges Government to Fix Critical Vulnerabilities in Three Days

Description

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has introduced a new directive, known as Binding Operational Directive 26-04. This directive aims to improve security measures for Federal Civilian Executive Branch (FCEB) agencies by addressing high-risk vulnerabilities more quickly.

CISA's objective is to reduce the risk of cyberattacks against the public sector. Under the new rules, agencies may need to resolve serious security vulnerabilities within as little as three days. This directive replaces older guidelines, BOD 19-02 and BOD 22-01, which were established in 2019 and 2021.

To decide the urgency of a patch, CISA considers four main factors. These include whether the asset is publicly accessible online, if the vulnerability appears in CISA’s Known Exploited Vulnerabilities (KEV) catalog, whether the system can be attacked on a large scale automatically, and if attackers might gain full control of a system.

If a vulnerability isn't immediately urgent, agencies will typically have two weeks to address it. The directive specifically targets information systems used by U.S. government departments but does not cover military systems or private contractors.

Agencies must revise their vulnerability management policies to align with this new directive. They have 60 days to implement necessary changes and up to 180 days to ensure ongoing monitoring and reporting of their systems.

Vocabulary List:

1. **directive** //dəˈrɛktɪv// (noun): an official order telling an organization what to do
2. **vulnerability** //ˌvʌlnərəˈbɪlɪti// (noun): a weak part that attackers can use
3. **Exploited** //ɪkˈsploɪtɪd// (adjective): used by attackers to take advantage of systems
4. **patch** //pætʃ// (noun): a small update to fix a problem
5. **implement** //ˈɪmpləmənt// (verb): to start using a plan or change
6. **monitoring** //ˈmɑnətərɪŋ// (noun): watching systems to find problems or attacks

Comprehension Questions

Multiple Choice

1. What is the purpose of Binding Operational Directive 26-04 introduced by CISA?

   Option: To improve security measures for FCEB agencies
   Option: To create new federal cybersecurity legislation
   Option: To deregulate cybersecurity policies
   Option: To enhance military cybersecurity protocols

2. How quickly may agencies need to address serious security vulnerabilities under the new directive?

   Option: Within one day
   Option: Within three days
   Option: Within a week
   Option: Within two weeks

3. Which of the following guidelines does the Binding Operational Directive 26-04 replace?

   Option: BOD 18-01
   Option: BOD 19-02 and BOD 22-01
   Option: BOD 20-03
   Option: BOD 21-01

4. What does CISA consider to decide the urgency of a patch?

   Option: Severity of the vulnerability
   Option: Number of users affected
   Option: Four main factors
   Option: Potential costs to agencies

5. Which systems are specifically targeted by the directive?

   Option: Military systems
   Option: Private contractor systems
   Option: Information systems used by U.S. government departments
   Option: All civilian systems

6. How many days do agencies have to implement necessary changes to align with the new directive?

   Option: 30 days
   Option: 45 days
   Option: 60 days
   Option: 90 days

True-False

7. CISA's objective is to increase the risk of cyberattacks against the public sector.

8. Agencies have two weeks to address vulnerabilities that are not immediately urgent.

9. The directive covers military systems and private contractors.

10. CISA's Known Exploited Vulnerabilities (KEV) catalog is one of the factors considered for urgency.

11. Agencies have up to 180 days to ensure ongoing monitoring and reporting of their systems.

12. BOD 26-04 was established in 2022.

Gap-Fill

13. CISA has introduced a new directive known as Binding Operational Directive 26-04 to address high-risk vulnerabilities for _____.

14. Agencies may need to resolve serious security vulnerabilities within as little as _____ days.

15. The directive requires agencies to revise their vulnerability management policies within _____ days.

16. CISA considers whether the asset is publicly accessible online, if it appears in the KEV catalog, and if attackers might gain _____ control of a system.

17. Under the new rules, if a vulnerability isn't immediately urgent, agencies will typically have _____ weeks to address it.

18. The directive specifies that ongoing monitoring and reporting of their systems should be ensured within _____ days.

Answer

Multiple Choice: 1. To improve security measures for FCEB agencies 2. Within three days 3. BOD 19-02 and BOD 22-01 4. Four main factors 5. Information systems used by U.S. government departments 6. 60 days
True-False: 7. False 8. True 9. False 10. True 11. True 12. False
Gap-Fill: 13. Federal Civilian Executive Branch (FCEB) agencies 14. three 15. 60 16. full 17. two 18. 180

CATEGORY

1. Business - LEVEL4

POST TAG

1. B2
2. CISA
3. ESL learning
4. esl news
5. exploited flaws
6. govt agencies
7. Level 4
8. patch

Tags

1. B2
2. CISA
3. ESL learning
4. esl news
5. exploited flaws
6. govt agencies
7. Level 4
8. patch

Date Created
2026/06/12
Author
aimeeyoung99