Date：2020/12/11

【Security Information】Internet security vendor FireEye red team security testing tool has been leaked. It is recommended to fix the CVE security vulnerabilities used by the tool as soon as possible!

Subject:【Security Information】Internet security vendor FireEye red team security testing tool has been leaked. It is recommended to fix the CVE security vulnerabilities used by the tool as soon as possible!

- Description:
  For details, please refer to the following links.
  1. http://cs-notices.fireeye.com/webmail/484561/315422185/88b9986cd9e2bb55e59d28a46b00470df398125330916b5dffa37f6b987de151
  2. https://github.com/fireeye/red_team_tool_countermeasures/blob/master/CVEs_red_team_tools.md
  3. https://github.com/fireeye/red_team_tool_countermeasures
- Impacted platform：
  1. CVE-2014-1812 – Windows Local Privilege Escalation
  2. CVE-2016-0167 – local privilege escalation on older versions of Microsoft Windows
  3. CVE-2017-11774 – RCE in Microsoft Outlook via crafted document execution (phishing)
  4. CVE-2018-8581 - Microsoft Exchange Server escalation of privileges
  5. CVE-2019-0604 – RCE for Microsoft Sharepoint
  6. CVE-2019-0708 – RCE of Windows Remote Desktop Services (RDS)
  7. CVE-2020-0688 – Remote Command Execution in Microsoft Exchange
  8. CVE-2020-1472 – Microsoft Active Directory escalation of privileges
  9. CVE-2019-8394 – arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDesk Plus
  10. CVE-2020-10189 – RCE for ZoHo ManageEngine Desktop Central
  11. CVE-2018-13379 – pre-auth arbitrary file reading from Fortinet Fortigate SSL VPN
  12. CVE-2018-15961 – RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)
  13. CVE-2019-3398 – Confluence Authenticated Remote Code Execution
  14. CVE-2019-11510 – pre-auth arbitrary file reading from Pulse Secure SSL VPNs
  15. CVE-2019-11580 - Atlassian Crowd Remote Code Execution
  16. CVE-2019-19781 – RCE of Citrix Application Delivery Controller and Citrix Gateway

---

Network System Division
Computer and Communication Center