

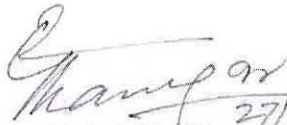
- 684

GOVERNMENT OF PAKISTAN
(REVENUE DIVISION)
FEDERAL BOARD OF REVENUE

Subject: CYBER SECURITY ADVISORY-ZERO DAY UNPATCHED MICROSOFT
OFFICE VULNERABILITY (ADVISORY NO. 63)

The undersigned is directed to enclose, herewith, a copy of self-explanatory letter No. 1-5/2003 (NTISB-II) dated 15th September, 2021 received from National Telecom & Information Technology Security Board (NTISB) Islamabad on the subject cited above for necessary action, please.

Encl: As above


(Abdul Ghaffar) 27/9/21
Second Secretary (Coord)

Secretary (IT), FBR

U.O. No. 6(2) Coord/Misc/2021

dated 27th September, 2021 155497-R

683

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad 15 September, 2021

Subject: Cyber Security Advisory – Zero Day Unpatched Microsoft Office Vulnerability
(Advisory No. 63)

1. A zero-day vulnerability has been identified that exploits Microsoft HTML through crafted Microsoft Office documents. This vulnerability effects all versions of MS Office and Windows Operating System. Through this vulnerability, an attacker can exploit end user by devising a malicious ActiveX control via crafted email or compromised websites. The maliciously crafted email once clicked by a user results in exploitation of endpoint. Microsoft has not yet released patch for this flaw. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned.

2. Forwarded for information / dissemination to all concerned, please.

M (IR-Ops)	
M (IR-P)	
M (Cus-Op)	
M (Cus-P)	
M (Admin)	✓
M (IT)	✓
M (FATE)	
M (Legal)	
M (Reforms)	
M (Legal & Acc. Cus)	
M (Acc. & Audit)	
Adl. Secy (Rev. Div.)	✓
SA / SPS	

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Secretary, Aviation Division, Islamabad
5. Additional Secretary-III, Cabinet Division, Islamabad
6. Director General (Tech), Dte Gen, ISI Islamabad
7. Secretary, NTISB, Cabinet Division, Islamabad
8. Deputy Secretary, NTISB, Cabinet Division, Islamabad
9. Director (IT), Cabinet Division, Islamabad

BR eCOX D. No. 135108-R

Received in Chairman's Office
17 SEP 2021

Cyber Security Advisory – Zero Day Unpatched Microsoft Office Vulnerability
(Advisory No. 63)

1. A Zero-Day vulnerability has been identified that exploits Microsoft HTML through crafted Microsoft Office documents. This vulnerability effects all versions of MS Office and Windows Operating System. Through this vulnerability, an attacker can exploit end user by devising a malicious Activex control via crafted email or compromised websites. The maliciously crafted email once clicked by a user results in exploitation of endpoint. Microsoft has not yet released patch for this flaw. Therefore, system / network administrators should follow recommendations mentioned at **Para 3** to avoid intrusions.

2. Technical Details

- a. Attack Vectors. Phishing Emails or Compromised Websites.
- b. Command / Utility Abused. MSHTML (software component used to render web pages on Windows).
- c. Vulnerability Index. CVE-2021-40444
- d. Patch details. Microsoft has not yet released an official patch for this vulnerability.

3. Recommendations

a. For System / Network Administrators

- (1) Windows commands / utilities not required at endusers **should be blacklisted for endpoint execution** like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe.
- (2) **Block execution of scripts** with .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif, .ps1 extensions.
- (3) Disable the installation of all ActiveX controls in Internet Explorer via the registry.
- (4) NW / System admins must ensure that all end user documents from the Internet are viewed in protected mode on all endpoints.
- (5) **Blacklist / Block outbound network connections** from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.
- (6) Centralized **Monitoring of endpoint windows logs** must be performed to detect anomalous user behavior.

- 888
- (7) Regularly update antimalware solutions running on endpoints in enterprise environment as well as standalone systems.
 - (8) Educate endusers regarding cyber security best practices and antimalware measures.

b. **For End-users**

- (1) **Regularly update antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.
- (2) **Do not download attachments from emails or websites unless it is received from trusted source.**
- (3) Avoid downloading softwares from untrusted websites or torrents.
- (4) Use Chrome / Firefox for browsing internet instead of Internet Explorer.
- (5) Make sure that web browser is up-to-date and no plugins other than Adblock or Adblock Plus is enabled.

4. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

5. Forwarded for perusal and dissemination of information to all concerned and under command, please.