

673 PRAL

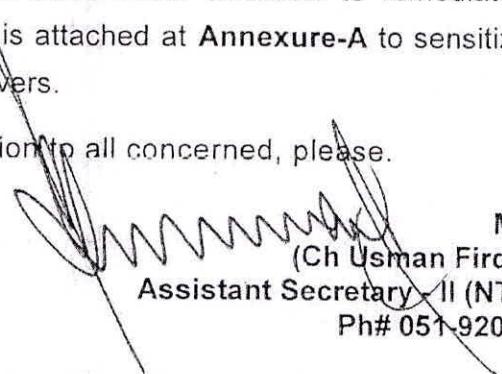
GOVERNMENT OF PAKISTAN
CABINET DIVISION, CABINET SECRETARIAT
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

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

Islamabad 29 September, 2021

Subject:- Cyber Security Advisory - Critical Vulnerabilities in vCenter Server (Advisory No. 65)

1. VMware vCenter Server is advanced server management software that provides a centralized platform for controlling VMware vSphere environment. On 22 September 2021, VMware has issued warning based on 19x critical vulnerabilities in the analytics service of vCenter Server. Updates have also been made available to remediate the existing vulnerabilities. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned for updating respective vCentre Servers.
2. Forwarded for information / dissemination to all concerned, please.


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. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

-692

Annexure-A

Cyber Security Advisory - Critical Vulnerabilities in vCenter Server (Advisory No. 65)

1. **Context.** VMware vCenter Server is an advanced server management software that provides a centralized platform for controlling VMware vSphere environment. On 22 September 2021, VMware has issued warning based on 19 x critical vulnerabilities in the analytics service of vCenter Server. Updates have also been made available to remediate the existing vulnerabilities.

2. **Affected Products.**

- a. VMware vCenter Server (VCenter Server)
- b. VMware Cloud Foundation (Cloud Foundation)

3. **Affected Products.**

- a. vCenter Server versions 6.7 and 7.0 are affected. vCenter 6.5 versions are found not affected

4. **Vulnerabilities**

Ser	CVE	Vulnerabilities Details
a.	CVE-2021-21991	vCenter Server local privilege escalation
b.	CVE-2021-21992	vCenter Server XML parsing denial-of-service
c.	CVE-2021-21993	vCenter Server SSRF
d.	CVE-2021-22005	vCenter file upload vulnerability network access to port 443
e.	CVE-2021-22006	vCenter Server reverse proxy bypass
f.	CVE-2021-22007	vCenter Server local information disclosure
g.	CVE-2021-22008	vCenter Server information disclosure
h.	CVE-2021-22009	vCenter Server VAPI multiple denial of service
i.	CVE-2021-22010	vCenter Server VPXD denial of service
j.	CVE-2021-22011	vCenter server unauthenticated API endpoint

k.	CVE-2021-22012	vCenter Server unauthenticated API information disclosure
l.	CVE-2021-22013	vCenter Server file path traversal
m.	CVE-2021-22014	vCenter Server authenticated code execution
n.	CVE-2021-22015	vCenter Server improper permission local privilege escalation
o.	CVE-2021-22016	vCenter Server reflected XSS
p.	CVE-2021-22017	vCenter Server rhttpproxy bypass
q.	CVE-2021-22018	vCenter Server file deletion
r.	CVE-2021-22019	vCenter Server denial of service
s.	CVE-2021-22020	vCenter Server Analytics service denial- of- service

5. **Recommendation.** The relevant patches at Para 4 may be downloaded from link:<https://www.vmware.com/security/advisories/VMSA-2021-0020.html>

6. **Reporting of Cyber Security Issues / Queries.** For reporting malware or any other query or issues regarding Cyber Security, details may please be forwarded to the following email addresses:-

"ntisb@cabinet.gov.pk "

7. Forwarded for compliance, please.