Pakistan Revenue Automation (Pvt) Ltd.

Plot #: 156, Software Technology Park
Service Road (North), Sector: I-9/3,
Islamabad
Ph. 051-9259435, Fax: 051-9259356

No. PRAL/CEO/ **2102/** 221043

Date: 19-02-2021

Ms. Rezwana Siddiqui
Chief (IT)
Federal Board of Revenue
Islamabad

Sub: ADVISORY – PREVENTION AGAINST VULNERABILITIES IN GOOGLE CHROME

Ref: Subject cited above.

Please find enclsoed Advisory Notice, which may be circulated within FBR with the purpose of creating precaution and data safeguard awareness among FBR officials.

2. As we are also receiving frequent advisories from Government security agencies, therefore it is suggested that the Advisory Notice may be posted online at FBR's website and also on the Notice Boards of FBR Offices.

3. Submitted for your information and further necessary action, please.

upload it

(Gohar Ahmed Khan)
Chief Executive Officer

Encl: As above.

PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

Friday, February 19, 2021

ADVISORY NOTICE

Prevention against Vulnerabilities in Google Chrome

Multiple vulnerabilities have been discovered in Google Chrome recently, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data.

If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

Systems Affected:
Google Chrome versions prior to 88.0.4324.182

Recommendations:

1. FBR IT Security Policy sanctioned by Member (IT) – FBR, must be strictly followed. A copy can be obtained from FBR IT Wing.
2. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. It is highly recommended that the computer system must be registered with LAN's Active Directory server. Please contact your local technical support for further details.
3. Avoid clicking unknown links and downloading attachments sent by anonymous users.
4. Use of third-party Antivirus is strictly prohibited. Only approved licensed Antivirus software must be installed on desktop PCs.
5. Always avoid using a suspicious USB flash stick. In case you still want to use the USB flash stick, then always scan the USB using approved Antivirus software.

6. Regular update Operating System, Antivirus software, Internet browsers, and MS Office, and disable macros.
7. Keep Windows firewall enabled on your desktop computer systems.
8. All sensitive information be handled with care and dissemination to all concerned be done through secure means.
9. Use of official email is highly recommended.
10. Change the passwords of your respective accounts regularly.
11. Always memorize the passwords, never write them.
12. Maintain regular offline backups or centralized offline backup of your critical data.
13. Be aware of pop-ups in internet browsers or desktop screens and never enter confidential information in a pop-up screen.
14. Contact your local PRAL technical support team for any assistance.
15. In case of infection/compromise in your computer system by your phone or other media, please disconnect the computer from the internet and immediately contact PRAL Technical Support Team.

Further information about online security threats and support, please contact PRAL Networks & Infrastructure Wing at:

Information & Support During Office Hours	
Landline	(051) 9259358
IP Phones	1234

Information & Extended Support 24x7	
Landline	(051) 9212374 (051) 8431155
IP Phones	1492 1155
Email	datacenter@pral.com.pk

Distribution to:

- FBR House, Islamabad
- All FBR IR & Custom Offices
- PRAL Head Office, Islamabad