Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 266 20-05-2024

Name: Multiple Intel Products Vulnerabilities

Threat Classification: Vulnerability

Affected Software / Services:

- Intel GPA Software
- Intel GPA Framework Software
- Intel Server Products UEFI Firmware
- Intel Server Board Onboard Video Driver Software

Summary:

A series of vulnerabilities have been identified in multiple Intel products, affecting Intel GPA Software, Intel GPA Framework Software, Intel Server Products UEFI Firmware, and Intel Server Board Onboard Video Driver Software. These vulnerabilities could allow local authenticated attackers to gain elevated privileges or cause a denial of service condition. The vulnerabilities range from incorrect default permissions to uncontrolled search paths and improper input validation.

Severity	**High**
Attack Vector	Local Privilege Escalation

CVE’s:

CVE-2023-24460	CVE-2023-35192	CVE-2023-41961	CVE-2023-43629
CVE-2023-40071	CVE-2024-21788	CVE-2023-43748	CVE-2024-21861
CVE-2024-22095	CVE-2023-42668	CVE-2024-23980	CVE-2024-23487
CVE-2023-22662	CVE-2024-22382	CVE-2024-24981	

Recommendations:

- Ensure users operate with the least privilege necessary to perform their job functions to minimize potential impact if an account is compromised.
- Implement comprehensive monitoring to detect any unusual activity that may indicate exploitation of these vulnerabilities.
- Limit physical and network access to systems running affected Intel products to trusted personnel only. Use multi-factor authentication (MFA) to further secure access.
- Perform regular security audits and vulnerability assessments to identify and remediate security weaknesses in your environment.
- Educate users about the risks of privilege escalation attacks and the importance of maintaining strong security hygiene, such as not reusing passwords and recognizing phishing attempts.
- Deploy HIDS to monitor critical files and directories for unauthorized changes, providing early warning of potential exploitation attempts.
- In case of any incident, please report to this office, through PTA CERT Portal and email.

Patch References:

For further details and the latest updates and patches, refer to Intel's Product Security Center (DGSSI) (CERT-FR)