NCA-16.240826 – National CERT Advisory

Malware Targeting Synchronized Passkeys on Compromised Windows Systems

A security risk has been identified in the implementation of synchronized passkey authentication on Windows systems. Security researchers have demonstrated that malware running on a compromised device can steal and misuse synchronized passkeys without requiring the victim's password, PIN, fingerprint, or other biometric authentication.

The identified weaknesses may allow attackers to authenticate as legitimate users and gain unauthorized access to accounts protected by passkeys. Although the underlying passkey cryptography remains secure, the attack exploits weaknesses in device trust and credential management on compromised endpoints.

Users and administrators are advised to apply security updates promptly, maintain strong endpoint security, and monitor for suspicious account activity to reduce the risk of compromise.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-16.240826
Threat Type	Credential Theft, Passkey Authentication Abuse, Persistent Unauthorized Account Access
Severity	High (Requires Prior Endpoint Compromise — Not Independently Rated in Source Advisory)
Attack Vector	Local exploitation via malware running on an already-compromised Windows endpoint, targeting Chrome Synced Passkey (Cloud Authenticator) storage
Authentication Required	Not applicable to the passkey theft step — attacker does not need the victim's password, PIN, or biometric once the endpoint is compromised
User Interaction	Not required for passkey theft once the device is compromised
CVSS Score	Not publicly disclosed in source advisory; no CVE identifier assigned
Scope & Applicability	Individual and organizational Google account holders using Google Chrome on Windows with Chrome Synced Passkeys (Cloud Authenticator) enabled
Affected Products	Google Chrome on Windows; Google accounts using Chrome Synced Passkeys (Cloud Authenticator); Windows systems compromised by malware

Security Advisory Source	Security researcher disclosure, as referenced in the source Cybersecurity Advisory Report dated 06 August 2026

IMPACT ANALYSIS

Successful exploitation of this vulnerability may allow attackers to:

1. Access online accounts protected by Google synced passkeys
2. Bypass password and biometric authentication on compromised devices
3. Steal passkey-related credentials from infected Windows systems
4. Maintain persistent unauthorized access to user accounts
5. Access sensitive personal or organizational information stored in affected accounts
6. Circumvent certain multi-factor authentication (MFA) protections
7. Increase the risk of identity theft and account compromise

THREAT CHARACTERISTICS

Field	Details
Threat Category	Credential Theft / Authentication Abuse (Synced Passkey Compromise)
Threat Status	Publicly demonstrated by security researchers; no confirmed in-the-wild exploitation reported in source advisory
Root Cause	Weaknesses in device trust and credential management on compromised Windows endpoints; underlying passkey cryptography remains secure, but synced passkey material can be stolen and misused once malware achieves device compromise
Attack Surface	Chrome Synced Passkey (Cloud Authenticator) storage and browser credential-handling processes on Windows
Attack Complexity	Medium requires the attacker to first achieve malware execution on the victim's Windows endpoint; passkey theft itself does not require victim credentials
Privileges Required	Local code execution on the victim's device (via malware); no victim password, PIN, or biometric required for the passkey theft step
Impact Scope	Unauthorized access to Google accounts protected by synced passkeys, potential MFA bypass, and persistent unauthorized account access

VULNERABILITY DETAILS

- Security researchers have demonstrated that malware running on a compromised Windows device can steal and misuse Chrome Synced Passkeys without requiring the victim's password, PIN, fingerprint, or other biometric authentication.

- The underlying passkey cryptography remains secure; the attack instead exploits weaknesses in device trust and credential management on already-compromised endpoints.
- Affected Component: Chrome Synced Passkeys (Cloud Authenticator) on Windows.
- Prerequisite: The attacker must first achieve malware execution on the victim's Windows endpoint before passkey theft is possible.

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should actively hunt for the following indicators within account activity logs, endpoint telemetry, and browser process monitoring:

1. Account & Authentication Indicators

- Unexpected account logins — sign-ins from unknown devices or locations using passkey authentication.
- Unauthorized passkey registration — new passkeys or trusted devices added without user knowledge.
- Unexpected account recovery or device onboarding — unexplained re-registration of trusted devices or passkeys.
- Security alerts from Google — notifications of new device sign-ins or suspicious account activity.

2. Endpoint & Browser Indicators

- Suspicious browser credential activity — unusual access to Chrome credential or passkey storage files.
- Malware detected on Windows endpoints — presence of information-stealing malware or credential theft tools.
- Abnormal Chrome process activity — unusual access to browser memory or cryptographic functions.

REMEDIATION ACTIONS

1. Immediate Defensive Controls

Action Category	Recommended Actions
Patch Management	Keep Google Chrome and Windows updated with the latest security patches.
Malware Scanning	Regularly scan systems for malware and remove any detected threats immediately.
Account Security Review	Review Google account security settings and monitor for unauthorized devices or passkeys.
Device De-authorization	Remove unknown or untrusted devices associated with Google accounts.

Privilege Restriction	Restrict administrative privileges and prevent unauthorized software installation.
User Awareness	Educate users about malware risks and safe browsing practices.
Incident Containment	Immediately isolate and investigate any system suspected of malware infection before using passkey-protected accounts.

2. Enhanced Monitoring & Detection

- Monitor for sign-ins from unknown devices or locations using passkey authentication.
- Track new passkey registrations or trusted device additions across Google accounts.
- Monitor for unusual access to Chrome credential or passkey storage files.
- Watch for abnormal Chrome process activity, including unexpected access to browser memory or cryptographic functions.

3. Incident Response Requirements

Organizations should:

- Immediately isolate and investigate any Windows system suspected of malware infection.
- Confirm and remove information-stealing malware or credential theft tools before restoring account access.
- Revoke and re-register passkeys and trusted devices for any account with confirmed or suspected compromise.
- Force re-authentication and review recent account activity for affected users.
- Preserve endpoint and account logs for forensic analysis where compromise is confirmed.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Patch Deployment	Apply the latest Google Chrome and Windows security updates.
Malware Remediation	Scan endpoints for malware and remove detected threats immediately.
Account Hardening	Remove unknown or untrusted devices and passkeys from Google accounts.
Threat Hunting	Monitor for the account, endpoint, and browser indicators listed above.
Incident Escalation	Report confirmed compromises to National CERT.

MONITORING & DETECTION REQUIREMENTS

1. Monitor for sign-ins from unknown devices or locations using passkey authentication.
2. Track new passkey registrations or trusted device additions.
3. Monitor unusual access to Chrome credential or passkey storage files.
4. Detect unexplained account recovery or device onboarding events.

5. Scan Windows endpoints for information-stealing malware or credential theft tools.
6. Monitor abnormal Chrome process activity, including browser memory or cryptographic function access.
7. Track Google security alerts for new device sign-ins or suspicious account activity.
8. Correlate endpoint malware detections with account-level anomalies.
9. Monitor for unauthorized administrative privilege use or unapproved software installation.
10. Track account access patterns for signs of persistent unauthorized access.

INCIDENT REPORTING

All suspected compromises, exploitation attempts, or anomalous activity related to this vulnerability must be immediately reported to National CERT Pakistan:

- Incident Reporting Portal: https://pkcert.gov.pk/report-incident/
- Email: cert@pkcert.gov.pk
- UAN: +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Apply the latest Google Chrome and Windows security updates immediately.
2	Scan all endpoints for malware and remove any detected threats.
3	Review Google account security settings for unauthorized devices or passkeys.
4	Remove unknown or untrusted devices associated with Google accounts.
5	Restrict administrative privileges and prevent unauthorized software installation.
6	Educate users on malware risks and safe browsing practices.
7	Isolate and investigate suspected compromised systems before using passkey-protected accounts.
8	Escalate confirmed compromises or indicators of exploitation to National CERT.