مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

DigiCert Certificate Revocation Incident

Tracking #:432316105

Date:31-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that DigiCert is revoking certificates due to improper Domain Control Verification (DCV) linked to missing underscore prefixes in DNS CNAME records

TECHNICAL DETAILS:

DigiCert is revoking certificates due to improper Domain Control Verification (DCV) linked to missing underscore prefixes in DNS CNAME records. Approximately 0.4% of domain validations were affected. All impacted customers must replace their certificates within 24 hours to maintain compliance with strict CABF regulations. According to an update on the related Bugzilla report, the incident impacts 83,267 certificates and 6,807 customers.

Recommendations:

1. **Immediate Certificate Replacement**:
   - Impacted customers must log into their DigiCert accounts to identify and reissue affected certificates within 24 hours.
2. **Review DNS Records**:
   - Validate that DNS CNAME records are correctly formatted with the required underscore prefix to avoid future validation issues.
3. **Monitor Updates from DigiCert**:
   - Regularly check the DigiCert status page for real-time updates and further instructions pertaining to this incident.
4. **Enhance Security Practices**:
   - Evaluate and enhance internal certificate lifecycle management and domain verification processes to better comply with CA/Browser Forum (CABF) requirements.
5. **Engage with Support**:
   - For any questions or support needs, proactively engage with DigiCert support channels for timely assistance.

Incident Details:

- **Cause of Revocation**:
  - Recent updates to DigiCert's validation system inadvertently omitted the underscore prefix in the CNAME record validation process, leading to non-compliance under CABF rules.

- **Regulatory Requirements**:
  - Under CABF guidelines, non-compliance with domain validation mandates immediate revocation of affected certificates within 24 hours.

- **Preventive Measures by DigiCert**:
  - DigiCert has committed to various actions to prevent a recurrence, including a consolidation of random value generators and compliance team involvement in review processes.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to stay informed on future updates from DigiCert and adjust processes accordingly to uphold compliance and security standards.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.digicert.com/support/certificate-revocation-incident