CONTINGENCY

Open Remote Desktop Web (RDWeb)

Coalition's Active Risk Platform continuously identifies vulnerabilities that may increase exposure to digital risks. By resolving these issues, organizations reduce the likelihood of adverse network events which commonly result in business disruptions and loss of critical business data to unauthorized threat actors.

Contingency Details

Remote Desktop Web, or RDWeb, facilitates remote access between systems through Remote Desktop Protocol over a web browser interface. When this remote access route is visible and accessible over the public Internet, it can be detected and targeted by unauthorized parties attempting to perform network intrusions.

Risk Rationale

Remote Desktop Protocol is well known as a leading attack vector for unauthorized network intrusions. Threat actors commonly scan the public internet for any accessible routes utilizing this protocol; when one is detected, it is vulnerable to brute force credential attacks. These are simple to conduct as RDP natively lacks strict security controls. Once successful access to the network is achieved, it is extremely easy to conduct more complex attack chains or propagate malware across the environment through lateral RDP connections. Historical data shows that multifactor authentication (MFA) is not sufficient to mitigate the threat this exposure poses, as attackers are increasingly phishing MFA credentials as well as usernames and passwords.

Recommendation

1. Disable the Remote Desktop Web interface or remove its ability to be accessed over the public internet.
    a. Extend any currently utilized network-layer controls to mitigate access to the RDWeb address. Restricting access to IP addresses contained within a company VPN is the most consistent access control, but a *web proxy solution* can also be deployed to similar effect.
    b. Alternatively you can use solutions such as Cloudflare Zero Trust or one of our recommended partners, Acreto, at a discount and free implementation. Click here to sign up and get help.
    c. Note that the implementation of MFA (Multi-factor authentication) does not mitigate the issue
2. Deploy an Endpoint Detection and Response (EDR) solution to 100% of endpoints
    a. Any EDR **except** the following is acceptable: Bitdefender, ESET Unified Threat Management, Kaspersky, Symantec, Webroot
    b. Coalition offers discounts on EDR vendors such as SentinelOne and MalwareBytes.
    c. Provide proof of deployment to Coalition Security or Underwriting contact

Potential impact(s)

Leaving RDWeb exposed to the open internet leaves your organization vulnerable to a wide range of security incidents.