ERT Threat Alert
Coronavirus: Security Recommendations For Remote Access Threats

March 18, 2020

To control the spread of the coronavirus (COVID-19), many organizations are requesting employees to work remotely. Doing so means leveraging enterprise virtual private networks (VPNs) and remote desktop solutions to connect to services.

This shift opens the door to an array of cybersecurity threats that specifically target these networks and solutions. Remote access solutions require organizations to expose a service from their premises and allow internet access to it, relying mostly on the security posture of the solution and the user identification solution it integrates with.

Service Disruption

As organizations now mostly depend on remote access for their day-to-day business, they need to take proactive measures to safeguard against threats and maintain continuity. Exposing critical services on the internet makes them vulnerable to service disruption by distributed denial-of-service (DDoS) attacks.

DDoS attacks can leverage many different sources to generate and send malicious traffic to the targeted victim. Volumetric attacks will try to consume all available bandwidth. Clean pipe solutions can provide relief in terms of bandwidth restrictions by using threshold filtering, but will typically not distinguish good from malicious traffic, and leave most remote users intermittently or indefinitely perturbed by the cyberattack.

A more insidious type of DDoS attack leverages intricacies in the protocol of the exposed services and targets specific weaknesses. Most enterprise VPN solutions and web services rely on Secure Socket Layer (SSL) or Transport Layer Security (TLS) to ensure the confidentiality of transmitted data, and in some cases, to verify and ensure the identity of both sides of the communication. Encrypted attacks can target the SSL handshake mechanism, send malicious data to the SSL server or abuse the SSL encryption key negotiation process. These attacks take advantage of the asymmetric resource requirements to perform SSL session handshakes. Each SSL session handshake consumes fifteen times more resources on the server compared to the client. This asymmetry allows attackers to bring down large infrastructures with limited resources. Since these attacks do not generate massive amounts of traffic, they are much harder to detect before the service is disrupted.

Recommendations to Protect Against Service Disruption

For continued availability of critical services, Radware recommends a hybrid DDoS solution combining both cloud-based DDoS services and on-premise protection to provide the best attack coverage and low latency. On-premise detection and mitigation will prevent disruption from application and protocol specific attacks, while providing automated diversion to the cloud as attack volume grows and the risk of network saturation increases.

Radware provides keyless protection against SSL-based DDoS attacks that preserve user privacy, add no latency and require no access to the organization's encryption keys.

Vulnerabilities

Over the past twelve months, remote access solutions have become increasingly controversial because enterprise VPNs have become the attack vector of choice for ongoing attacks from advanced persistent threat (APT) actors. Microsoft's remote desktop solution, based on the Remote Desktop Protocol (RDP), was the subject of a National Security Agency warning (based on research) revealing that just under one million internet-facing machines were vulnerable to the BlueKeep vulnerability. RDP has also been the preferred attack vector for ransomware for years. According to research conducted by Coveware, RDP was the attack vector used by every two out of three ransomwares.

More recently, Citrix Access Gateway and application delivery controller were affected by a path traversal vulnerability for which there was no fix. In addition, an exploit was published allowing remote attackers to gain access to internal networks within a minute before the general availability of a fix.

Enterprise VPN Vulnerabilities

Last year, vulnerabilities allowing remote attackers to take control of an affected system and get unrestricted access to the internal network were discovered in VPN products from Palo Alto Networks, Fortinet and Pulse Secure. Alerts and warnings were issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Centre (NCSC) urging administrators to review and update their respective VPN solutions.

- Palo Alto Network Security Advisory PAN-SA-2019-0020, in relation to CVE-2019-1579
- FortiGuard Security Advisories FG-IR-18-389, in relation to CVE-2018-13382; FG-IR-18-388 in relation to CVE-2018-13383; FG-IR-18-384, in relation to CVE-2018-13379;
- Pulse Secure Security Advisory SA44101, in relation to CVE-2019-11510, CVE-2019-11508, CVE-2019-11540, CVE-2019-11543, CVE-2019-11541, CVE-2019-11542, CVE-2019-11539, CVE-2019-11538, CVE-2019-11509, CVE-2019-11507

To detect exploitation attempts of Pulse Connect Secure, the NCSC advises users have web request logging enabled and to inspect logs for evidence of exploitation as described in the table below.

Vulnerability	Detection
CVE-2019-11510	Search logs for URLs containing ? and ending with /dana/html5acc/guacamole/ (Regular Expression: \?.*dana/html5acc/guacamole/)<br />If any are found dated before the patch was applied, it may indicate a compromise. The matching string will contain the name of the file the attacker attempted to read.
CVE-2019-11539	Search for requests to /dana-admin/diag/diag.cgi with an options= parameter in the URL. An exploit will almost certainly contain: -r, # or 2><br/>Data between -r and # is Perl code that would be executed.

Fortigate devices do not log web requests by default, but if a device is configured to write firewall logs for all connections, or if firewall or Netflow logs are available from another device, it might be possible to detect exploitation. When exploiting CVE-2018-13379, an attacker may download a file called “sslvpn_websession,” which contains usernames and passwords of active users. This file is typically at least 200Kb. Firewall or netflow logs can be inspected for TCP sessions with 200,000-250,000 bytes emerging from the SSL VPN web interface port to the remote attacker.

In Palo Alto devices, it may be difficult to detect past exploitations in logs, but failed exploit attempts may cause a crash, which in turn could be visible in the logs.

Citrix

In December of 2019, Citrix announced a vulnerability (CVE-2019-19781) in their Citrix Application Delivery Controller (ADC) and Citrix SD-WAN WANOP appliance. The scope of the vulnerability included Citrix ADC and Citrix Gateway Virtual Appliances (VPX) hosted on any of Citrix Hypervisor, ESX, Hyper-V, KVM, Azure, AWS, GCP or on a Citrix ADC Service Delivery Appliance (SDX). The issue also affected certain deployments of Citrix SD-WAN, specifically Citrix SD-WAN WANOP edition, which packages Citrix ADC as a load balancer.

At the time of disclosure, there was no fix for the vulnerability. Only limited mitigation options were provided by Citrix, creating significant controversy within the infosec community which codenamed the vulnerability "Shitrix." By January, public proof-of-concept exploit code was released allowing attackers to take over devices and access an organization's internal network within a minute.

Researchers estimated that at least 80,000 organizations in 158 countries were at risk from this vulnerability, which could allow a remote attacker to compromise an internal network. Some researchers recommended the ultimate solution: power off or disconnect the devices until a fix is made available. By the end of January 2020, Citrix provided updates for all supported versions of their affected products.

The CISA provides multiple detection methods to find potential exploits of CVE-2019-19781. Since the impacted Citrix products utilize Apache for web server software, HTTP access and error logs are available on the system for review in **/var/log**. Log files httpaccess.log and httperror.log should both be reviewed for the following Uniform Resource Identifiers (URIs):

```
*/../vpns/*
*/vpns/cfg/smb.conf
*/vpns/portal/scripts/*.pl*
```

Signs of successful exploitation would be a POST request to a URI containing /../ or /vpn**,** followed by a GET request to an XML file. TrustedSec's blog provided sample logs indicating what a successful attack would look like:

```
10.1.1.1 - - [10/Jan/2020:13:23:51 +0000] "POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 200
143 "https://10.1.1.2/" "USERAGENT "

10.1.1.1 - - [10/Jan/2020:13:23:53 +0000] "GET /vpn/../vpns/portal/backdoor.xml HTTP/1.1" 200 941 "-"
"USERAGENT"
```

Recommendations to Protect Against VPN Vulnerabilities

Radware recommends:

- Updating VPNs, network infrastructure devices and devices being used to work remotely with the latest software patches
- Implement multi-factor authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords and not reuse passwords for other purposes or sites
- Reset credentials associated with potentially affected VPNs
- Implement granular access controls in VPN solutions to limit the access based on user profiles
- Ensure and enforce the security posture of client devices before allowing access to internal resources

BlueKeep

In May of 2019, Microsoft released fixes for a critical remote code execution (RCE) vulnerability in their Remote Desktop Services, formerly known as Terminal Services, referred to by CVE-2019-0708. The vulnerability was privately reported to Microsoft by the NCSC and affects older versions of Windows.

Microsoft stated it was confident that there was already an exploit for this vulnerability and that it could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware. An internet-scale port scanner determined that there were almost one million internet-facing machines vulnerable to BlueKeep on port 3389 in May 2019.

By August 2019, a security researcher under the Twitter handle @zerosum0x0 disclosed his RDP exploit for the BlueKeep vulnerability to Metasploit. It is expected to increase the amount of RDP scanning activity and attempted exploitations of any unpatched systems exposed on the internet.

Affected Windows versions include Windows Server 2003, 2008 and 2008 R2, as well as Windows 7, XP and Vista. Windows 8 and Windows 10 are not impacted by the vulnerability.

Recommendation to Protect Against BlueKeep

Updates were provided as part of Microsoft's automated update process in May 2019. A list of security updates and knowledge base articles for all the affected Windows systems is available from Microsoft.

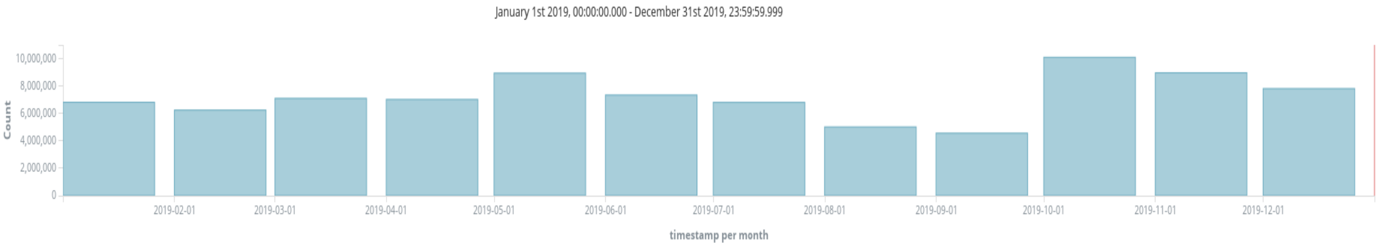
DefensePro customers have a specific signature that protects them from known BlueKeep attacks as part of their Security Update Signature subscription. The signature is referenced as RWID 18944: RDP-MS-T120-CHANNEL-VER1-RCE (CVE-2019-0708)**.**

RDP Account Takeover Attacks (ATO)

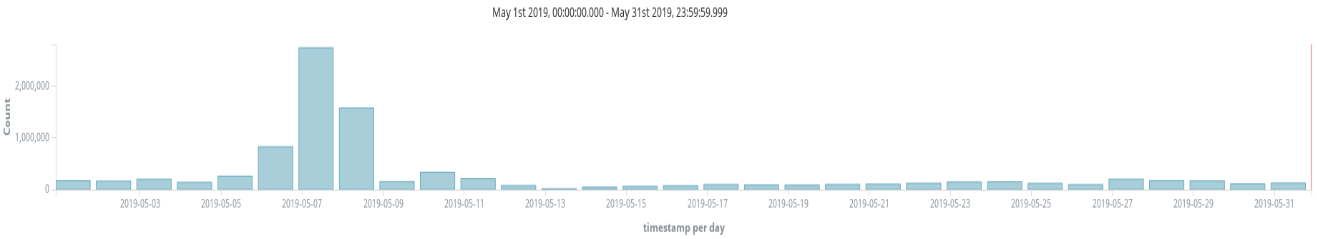
Around 0.08% of RDP Brute Force attacks are successful and these attacks last two to three days, according to a recent Microsoft report presenting the results of a study into the impact of RDP Brute Force attacks on the enterprise sector. RDP credentials are a regular item on underground trading sites. Prices vary between $8 to $15 based on country and type of operating system. The harvesting of RDP credentials, also referred to as account takeover attacks, can leave users perturbated or unable to access the service.

Malicious RDP Scanning Activity

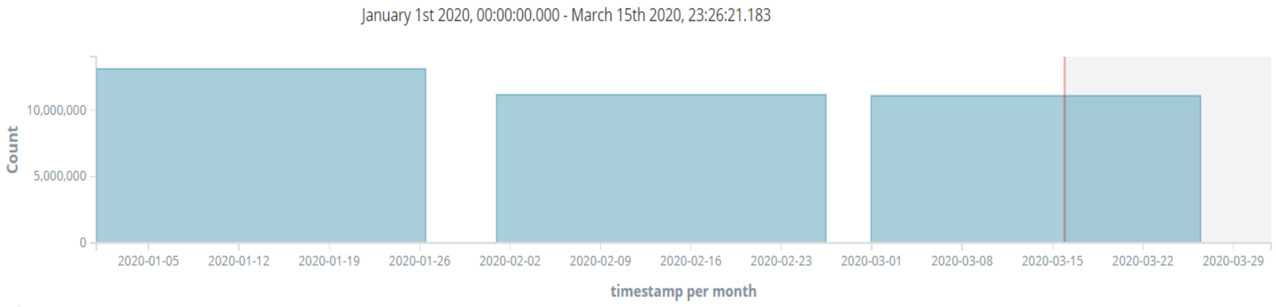
The overall RDP activity, as recorded by Radware's deception network, confirms the urge for protecting against RDP attacks. Throughout 2019, nearly 87 million events were recorded in our RDP deception service, averaging 240,000 malicious events per day.



On May 7, 2019, the largest peak of the year was recorded with over 2.5 million scans. This is equivalent to 100,000 scans per hour and coincides with the timeframe of the BlueKeep vulnerability disclosure.



Malicious activity continues this year with almost 35 million malicious attempts recorded to date, or an average of 10 million attempts per day.



Recommendations to Protect Against RDP ATO Attacks

To protect against RDP account takeovers, Microsoft recommends that system administrators combine and monitor multiple signals that can detect RDP inbound Brute Force traffic on their servers.

- Hour of day and day of week of failed sign-in and RDP connections
- Timing of successful sign-in following failed attempts
- Event ID 4625 login type (filtered to network and remote interactive)
- Event ID 4625 failure reason (filtered to %%2308, %%2312, %%2313)
- Cumulative count of distinct usernames that failed to sign in without success
- Count (and cumulative count) of failed sign-ins
- Count (and cumulative count) of RDP inbound external IP

View Radware's Business Continuity Plan

- Count of other machines having RDP inbound connections from one or more of the same IP

Radware's ERT Active Attacker Feed provides proactive protection against scans and attacks from most malicious devices and servers recorded in our deception network.

To protect against any impact on the quality of the rendered service by Brute Force attacks, Radware recommends leveraging traffic filters on DefensePro to limit the number of new sessions to the RDP services.

Phishing

Fear and a need for information provides a breeding ground for cyber scams and abuse. Many phishing campaigns have been discovered since the coronavirus became a pandemic. Most scams are luring people with the promise of important or breaking information on COVID-19, enticing them to click malicious links or open infected attachments.

Recommendations to Protect Against Phishing Attacks

Stay current with anti-malware and phishing products and inform employees about the dangers of opening attachments or clicking links in emails from untrusted sources. While most organizations already implement a general awareness program for phishing, it does not hurt to inform employees about an expected increase in phishing attempts promising information on COVID-19.

Common Vulnerabilities and Exposures

CVE-ID	Description	Product Vendor
CVE-2019-1579	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.	PAN
CVE-2018-13379	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.	Fortinet
CVE-2018-13382	An Improper Authorization vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to 5.4.10 under SSL VPN web portal allows an unauthenticated attacker to modify the password of an SSL VPN web portal user via specially crafted HTTP requests.	Fortinet
CVE-2018-13383	A heap buffer overflow in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.10, 5.4.0 to 5.4.12, 5.2.14 and below in the SSL VPN web portal may cause the SSL VPN web service termination for logged in users due to a failure to properly handle javascript href data when proxying webpages.	Fortinet
CVE-2019-11510	In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.	Pulse Secure

CVE-2019-11508	In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an authenticated attacker (via the admin web interface) can exploit Directory Traversal to execute arbitrary code on the appliance.	Pulse Secure
CVE-2019-11540	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4 and 8.3RX before 8.3R7.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2 and 5.4RX before 5.4R7.1, an unauthenticated, remote attacker can conduct a session hijacking attack.	Pulse Secure
CVE-2019-11543	XSS exists in the admin web console in Pulse Secure Pulse Connect Secure (PCS) 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, and 5.2RX before 5.2R12.1.	Pulse Secure
CVE-2019-11541	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.2RX before 8.2R12.1, users using SAML authentication with the Reuse Existing NC (Pulse) Session option may see authentication leaks.	Pulse Secure
CVE-2019-11542	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, an authenticated attacker (via the admin web interface) can send a specially crafted message resulting in a stack buffer overflow.	Pulse Secure
CVE-2019-11539	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, the admin web interface allows an authenticated attacker to inject and execute commands.	Pulse Secure
CVE-2019-11538	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1, an NFS problem could allow an authenticated attacker to access the contents of arbitrary files on the affected device.	Pulse Secure
CVE-2019-11509	In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4 and Pulse Policy Secure (PPS) before 5.1R15.1, 5.2 before 5.2R12.1, 5.3 before 5.3R15.1, 5.4 before 5.4R7.1, and 9.0 before 9.0R3.2, an authenticated attacker (via the admin web interface) can exploit Incorrect Access Control to execute arbitrary code on the appliance.	Pulse Secure
CVE-2019-11507	In Pulse Secure Pulse Connect Secure (PCS) 8.3.x before 8.3R7.1 and 9.0.x before 9.0R3, an XSS issue has been found on the Application Launcher page.	Pulse Secure
CVE-2019-0708	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	Microsoft

CVE-2019-19781	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	Citrix

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

View Radware's Business Continuity Plan