ОТЧЕТ ОБ АНАЛИЗЕ УЯЗВИМОСТЕЙ

Организация:	ООО 'ТехноПром'
Дата сканирования:	2024-05-05 10:00:00
Дата генерации отчета:	2025-05-05 15:16:49
Сгенерировано:	SecFlash Vulnerability Scanner

Конфиденциально

Только для внутреннего использования

КРАТКОЕ СОДЕРЖАНИЕ

В ходе анализа сети было обнаружено 1213 уязвимостей на 5 хостах. Распределение по критичности: • Критические: 0 • Высокие: 0 • Средние: 0 • Низкие: 0 • Неизвестно (N/A): 1213 Наиболее опасные уязвимости: • Отсутствуют критические или высокие уязвимости

ДЕТАЛЬНЫЙ ОТЧЕТ ОБ УЯЗВИМОСТЯХ

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2007-4723	N/A	N/A	Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass auth...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2009-0796	N/A	N/A	Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, whe...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2009-2299	N/A	N/A	The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2011-1176	N/A	N/A	The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2011-2688	N/A	N/A	SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attack...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2012-3526	N/A	N/A	The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2012-4001	N/A	N/A	The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger ...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2012-4360	N/A	N/A	Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2013-0941	N/A	N/A	EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before ...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2013-0942	N/A	N/A	Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7....

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2013-2765	N/A	N/A	The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2013-4365	N/A	N/A	Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server ...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2021-41524	N/A	7.5	While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the s...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2021-41773	N/A	7.5	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to fil...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2021-42013	N/A	9.8	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs ...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2021-44224	N/A	8.2	A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixin...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2021-44790	N/A	9.8	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-22719	N/A	7.5	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Serve...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-22720	N/A	9.8	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server t...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-22721	N/A	9.1	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later cau...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-23943	N/A	9.8	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. T...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-26377	N/A	7.5	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-28330	N/A	5.3	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-28614	N/A	5.3	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-28615	N/A	9.1	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extreme...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-29404	N/A	7.5	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no defaul...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-30556	N/A	7.5	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the b...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-31813	N/A	9.8	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop me...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2006-20001	N/A	7.5	A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header val...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-36760	N/A	9.0	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smu...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2022-37436	N/A	5.3	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorpor...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2023-25690	N/A	9.8	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affect...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2023-27522	N/A	7.5	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. S...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2023-31122	N/A	7.5	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2023-45802	N/A	5.9	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. In...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-27316	N/A	7.5	HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client doe...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-38474	N/A	9.8	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-38475	N/A	9.1	Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are pe...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-38476	N/A	9.8	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend ap...
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-38477	N/A	7.5	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users a...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	Apache httpd 2.4.49	CVE-2024-40898	N/A	7.5	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF ...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2009-1390	N/A	N/A	Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the c...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2009-3765	N/A	N/A	mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (C...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2009-3766	N/A	N/A	mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) fi...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2009-3767	N/A	N/A	libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\0' character in a d...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2018-0735	N/A	5.9	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2018-0734	N/A	5.9	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing a...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-0190	N/A	7.5	A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to en...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1543	N/A	7.4	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) sh...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1552	N/A	3.3	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This d...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1547	N/A	4.7	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is pos...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1549	N/A	5.3	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event of a fork() system call in or...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1563	N/A	3.7	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very la...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2019-1551	N/A	5.3	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analys...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2020-1971	N/A	5.9	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL prov...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-23840	N/A	7.5	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is clo...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-23841	N/A	5.9	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contai...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-3449	N/A	5.9	An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-3711	N/A	9.8	In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-3712	N/A	7.4	ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holdin...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2021-4160	N/A	5.9	There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default c...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-0778	N/A	7.5	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally th...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-1292	N/A	9.8	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-2068	N/A	9.8	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly san...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-2097	N/A	5.3	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumst...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-4304	N/A	5.9	A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2022-4450	N/A	7.5	The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload dat...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-0215	N/A	7.5	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to suppo...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-0286	N/A	7.4	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRIN...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-0464	N/A	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that includ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-0465	N/A	5.3	Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-0466	N/A	5.3	The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. Howe...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-2650	N/A	6.5	Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-4807	N/A	7.8	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on t...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2023-5678	N/A	5.3	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: A...
192.168.1.10	80, 443, 22	OpenSSL 1.1.1	CVE-2024-0727	N/A	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summar...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2000-0143	N/A	N/A	The SSH protocol server sshd allows local users without shell access to redirect a TCP connection through a service that uses the standard system pass...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2001-0529	N/A	N/A	OpenSSH version 2.9 and earlier, with X forwarding enabled, allows a local attacker to delete any file named 'cookies' via a symlink attack.
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2001-1382	N/A	N/A	The "echo simulation" traffic analysis countermeasure in OpenSSH before 2.9.9p2 sends an additional echo packet after the password and carriage return...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2001-1380	N/A	N/A	OpenSSH before 2.9.9, while using keypairs and multiple keys of different types in the ~/.ssh/authorized_keys2 file, may not properly handle the "from...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2001-0816	N/A	N/A	OpenSSH before 2.9.9, when running sftp using sftp-server and using restricted keypairs, allows remote authenticated users to bypass authorized_keys2 ...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2001-0872	N/A	N/A	OpenSSH 3.0.1 and earlier with UseLogin enabled does not properly cleanse critical environment variables such as LD_PRELOAD, which allows local users ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2003-0190	N/A	N/A	OpenSSH-portable (OpenSSH) 3.6.1p1 and earlier with PAM support enabled immediately sends an error message when a user does not exist, which allows re...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2003-0693	N/A	N/A	A "buffer management error" in buffer_append_space of buffer.c for OpenSSH before 3.7 may allow remote attackers to execute arbitrary code by causing ...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2003-0682	N/A	N/A	"Memory bugs" in OpenSSH 3.7.1 and earlier, with unknown impact, a different set of vulnerabilities than CVE-2003-0693 and CVE-2003-0695.
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2003-0695	N/A	N/A	Multiple "buffer management errors" in OpenSSH before 3.7.1 may allow attackers to cause a denial of service or execute arbitrary code using (1) buffe...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2004-1653	N/A	N/A	The default configuration for OpenSSH enables AllowTcpForwarding, which could allow remote authenticated users to perform a port bounce, when configur...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2006-5051	N/A	8.1	Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2006-5794	N/A	N/A	Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been succe...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2007-2768	N/A	N/A	OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, whic...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2007-4752	N/A	N/A	ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows atta...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2008-3259	N/A	N/A	OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some pl...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2008-3844	N/A	N/A	Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an external...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2008-4109	N/A	N/A	A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch; before 4.6p1-1 on sid and lenny; and on other distributions such as SUSE uses function...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2010-4478	N/A	N/A	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attacker...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2010-4755	N/A	N/A	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, Net...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2012-0814	N/A	N/A	The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, wh...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2011-5000	N/A	N/A	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authentica...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2010-5107	N/A	N/A	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2014-1692	N/A	N/A	The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2011-4327	N/A	N/A	ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2014-2532	N/A	4.9	sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended env...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2014-2653	N/A	N/A	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR ch...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2014-9278	N/A	N/A	The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos environment, allows remote authenticated users to ...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2015-5352	N/A	N/A	The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadlin...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2015-5600	N/A	N/A	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2015-6563	N/A	N/A	The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, wh...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2015-6564	N/A	N/A	Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow lo...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-10009	N/A	7.3	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modul...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-10010	N/A	7.0	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gai...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-10011	N/A	5.5	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-10012	N/A	7.8	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforc...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-1908	N/A	9.8	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-contro...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2017-15906	N/A	5.3	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers t...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-10708	N/A	7.5	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEW...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2018-15473	N/A	5.3	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2018-20685	N/A	5.3	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. T...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2019-6109	N/A	6.8	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2019-6110	N/A	6.8	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipu...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2019-6111	N/A	5.9	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2020-15778	N/A	7.8	scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argume...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2016-20012	N/A	5.3	OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to ...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2021-36368	N/A	3.7	An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, an...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2023-38408	N/A	9.8	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent i...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2023-48795	N/A	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrit...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2023-51385	N/A	6.5	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2023-51767	N/A	7.0	OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authe...
192.168.1.10	80, 443, 22	OpenSSH 8.2p1	CVE-2024-6387	N/A	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2013-3900	N/A	5.5	Why is Microsoft republishing a CVE from 2013? We are republishing CVE-2013-3900 in the Security Update Guide to update the Security Updates table and...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8320	N/A	4.3	A security feature bypass vulnerability exists in DNS Global Blocklist feature, aka "Windows DNS Security Feature Bypass Vulnerability." This affects ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8330	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8333	N/A	7.0	An Elevation of Privilege vulnerability exists in Filter Manager when it improperly handles objects in memory, aka "Microsoft Filter Manager Elevation...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8411	N/A	7.8	An elevation of privilege vulnerability exists when NTFS improperly checks access, aka "NTFS Elevation of Privilege Vulnerability." This affects Windo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8413	N/A	7.8	A remote code execution vulnerability exists when "Windows Theme API" does not properly decompress files, aka "Windows Theme API Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8423	N/A	7.8	A remote code execution vulnerability exists in the Microsoft JET Database Engine, aka "Microsoft JET Database Engine Remote Code Execution Vulnerabil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8432	N/A	7.8	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka "Microsoft Graphics Component...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8453	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8460	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8472	N/A	5.5	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an atta...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8473	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8481	N/A	3.1	An information disclosure vulnerability exists when Windows Media Player improperly discloses file information, aka "Windows Media Player Information ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8482	N/A	3.1	An information disclosure vulnerability exists when Windows Media Player improperly discloses file information, aka "Windows Media Player Information ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8484	N/A	7.8	An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objects in memory, aka "DirectX Gr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8486	N/A	5.5	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Information Disclosure Vulnerability." ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8489	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8490	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8491	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8492	N/A	5.3	A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8494	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka "MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8497	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka "Windows Kernel Elevation of Privileg...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8503	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8505	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8506	N/A	5.5	An Information Disclosure vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka "Microsoft Windows Code...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8510	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8511	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8513	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-17612	N/A	7.5	Sennheiser HeadSetup 7.3.4903 places Certification Authority (CA) certificates into the Trusted Root CA store of the local system, and publishes the p...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8256	N/A	8.8	A remote code execution vulnerability exists when PowerShell improperly handles specially crafted files, aka "Microsoft PowerShell Remote Code Executi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8407	N/A	5.5	An information disclosure vulnerability exists when "Kernel Remote Procedure Call Provider" driver improperly initializes objects in memory, aka "MSRP...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8415	N/A	7.8	A tampering vulnerability exists in PowerShell that could allow an attacker to execute unlogged code, aka "Microsoft PowerShell Tampering Vulnerabilit...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8417	N/A	5.3	A security feature bypass vulnerability exists in Microsoft JScript that could allow an attacker to bypass Device Guard, aka "Microsoft JScript Securi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8454	N/A	5.5	An information disclosure vulnerability exists when Windows Audio Service fails to properly handle objects in memory, aka "Windows Audio Service Infor...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8471	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Microsoft RemoteFX Virtual GPU miniport driver handles objects in memory, aka "Micr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8476	N/A	9.8	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory, aka "Windows Deploymen...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8485	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Elevation of Privilege Vulnerability." ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8541	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8542	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8543	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8544	N/A	8.8	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8545	N/A	4.3	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka "Microsoft Edge Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8547	N/A	5.4	A cross-site-scripting (XSS) vulnerability exists when an open source customization for Microsoft Active Directory Federation Services (AD FS) does no...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8549	N/A	5.5	A security feature bypass exists when Windows incorrectly validates kernel driver signatures, aka "Windows Security Feature Bypass Vulnerability." Thi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8550	N/A	7.8	An elevation of privilege exists in Windows COM Aggregate Marshaler, aka "Windows COM Elevation of Privilege Vulnerability." This affects Windows 7, W...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8551	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8552	N/A	7.5	An information disclosure vulnerability exists when VBScript improperly discloses the contents of its memory, which could provide an attacker with inf...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8554	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Elevation of Privilege Vulnerability." ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8555	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8556	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8557	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8561	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Elevation of Privilege Vulnerability." ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8562	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8564	N/A	4.3	A spoofing vulnerability exists when Microsoft Edge improperly handles specific HTML content, aka "Microsoft Edge Spoofing Vulnerability." This affect...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8566	N/A	4.6	A security feature bypass vulnerability exists when Windows improperly suspends BitLocker Device Encryption, aka "BitLocker Security Feature Bypass Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8582	N/A	8.8	A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially modified rule export files, aka "Microsoft Outlook Rem...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8584	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC), aka "Windows ALPC Elevat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8588	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8592	N/A	6.4	An elevation of privilege vulnerability exists in Windows 10 version 1809 when installed from physical media (USB, DVD, etc, aka "Windows Elevation Of...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8477	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8514	N/A	5.5	An information disclosure vulnerability exists when Remote Procedure Call runtime improperly initializes objects in memory, aka "Remote Procedure Call...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8517	N/A	7.5	A denial of service vulnerability exists when .NET Framework improperly handles special web requests, aka ".NET Framework Denial Of Service Vulnerabil...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8540	N/A	9.8	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka ".NET Framework Remote Code Injec...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8583	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8595	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8596	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8599	N/A	7.8	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, ak...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8611	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka "Windows Kernel Elevation of Pr...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8612	N/A	5.5	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values, aka "Connect...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8617	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8618	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8619	N/A	7.5	A remote code execution vulnerability exists when the Internet Explorer VBScript execution policy does not properly restrict VBScript under specific c...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8624	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8625	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code E...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8626	N/A	9.8	A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests, aka "Windows DNS ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8629	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8631	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8634	N/A	8.8	A remote code execution vulnerability exists in Windows where Microsoft text-to-speech fails to properly handle objects in the memory, aka "Microsoft ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8637	N/A	5.5	An information disclosure vulnerability exists in Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Addr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8638	N/A	5.5	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Information Disclosure Vulnerability." ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8639	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8641	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka "Win32k ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8643	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8649	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka "Windows Denial of Service Vulnerability." This affect...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2018-8653	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0536	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0538	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0539	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0541	N/A	8.8	A remote code execution vulnerability exists in the way that the MSHTML engine inproperly validates input, aka "MSHTML Engine Remote Code Execution Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0543	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka "Microsoft Windows Elevation of Privilege ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0545	N/A	7.5	An information disclosure vulnerability exists in .NET Framework and .NET Core which allows bypassing Cross-origin Resource Sharing (CORS) configurati...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0549	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0550	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0551	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0552	N/A	8.8	An elevation of privilege exists in Windows COM Desktop Broker, aka "Windows COM Elevation of Privilege Vulnerability." This affects Windows Server 20...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0553	N/A	5.5	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka "Windows Subsystem for Linux...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0554	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0555	N/A	7.8	An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0565	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0566	N/A	8.8	An elevation of privilege vulnerability exists in Microsoft Edge Browser Broker COM object, aka "Microsoft Edge Elevation of Privilege Vulnerability."...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0567	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0568	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0569	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0570	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka "Windows Runtime Elevation of Privil...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0571	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0572	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0573	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0574	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0575	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0576	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0577	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0578	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0579	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0580	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0581	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0582	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0583	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0584	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0590	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0591	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0593	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0595	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0596	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0597	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0598	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0599	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0600	N/A	4.7	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Informa...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0601	N/A	4.7	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Informa...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0602	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0605	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0606	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0607	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0610	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0613	N/A	8.8	A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0615	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0616	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0618	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0619	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0621	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0625	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0626	N/A	9.8	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Wi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0627	N/A	7.8	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass V...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0628	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0630	N/A	8.8	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0631	N/A	7.8	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0632	N/A	7.8	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0633	N/A	8.8	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0634	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerab...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0635	N/A	6.2	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0636	N/A	5.5	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0637	N/A	7.5	A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections, a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0640	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0641	N/A	5.9	A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting, aka 'Microsoft Edge Security Feature Bypass Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0642	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0643	N/A	4.3	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0644	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0645	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0648	N/A	4.3	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with infor...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0649	N/A	8.1	A vulnerability exists in Microsoft Chakra JIT server, aka 'Scripting Engine Elevation of Privileged Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0650	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerab...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0651	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0652	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0654	N/A	4.3	A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects, aka 'Microsoft Browser Spoofing Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0655	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0656	N/A	7.0	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0657	N/A	5.9	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0658	N/A	6.5	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0659	N/A	7.0	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0660	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0662	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0676	N/A	6.5	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.An attacker who successfully exploited this...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0592	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0603	N/A	7.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who succes...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0609	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0611	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0612	N/A	5.3	A security feature bypass vulnerability exists when Click2Play protection in Microsoft Edge improperly handles flash objects. By itself, this bypass v...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0614	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0617	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0639	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0665	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0666	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0667	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0678	N/A	6.8	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0680	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0682	N/A	7.8	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation o...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0689	N/A	7.8	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation o...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0690	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0692	N/A	7.8	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation o...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0693	N/A	7.8	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation o...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0694	N/A	7.8	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation o...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0695	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0696	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0697	N/A	9.8	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0698	N/A	9.8	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0701	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0702	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0703	N/A	6.5	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0704	N/A	6.5	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0726	N/A	9.8	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0746	N/A	6.5	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0754	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0755	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0756	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0759	N/A	5.5	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler I...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0761	N/A	6.5	A security feature bypass vulnerability exists when Internet Explorer fails to validate the correct Security Zone of requests for specific URLs, aka '...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0762	N/A	4.3	A security feature bypass vulnerability exists when Microsoft browsers improperly handle requests of different origins, aka 'Microsoft Browsers Securi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0763	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0765	N/A	8.8	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0766	N/A	7.8	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vuln...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0767	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an auth...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0768	N/A	4.3	A security feature bypass vulnerability exists when Internet Explorer VBScript execution policy does not properly restrict VBScript under specific con...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0769	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0771	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0772	N/A	8.8	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0773	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0774	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0775	N/A	4.7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0776	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0780	N/A	7.5	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0782	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0783	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0784	N/A	7.5	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Cod...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0797	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0821	N/A	6.5	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0685	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0688	N/A	7.5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0730	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privil...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0731	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0732	N/A	7.8	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls t...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0735	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0739	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine M...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0752	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0753	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0764	N/A	6.5	A tampering vulnerability exists when Microsoft browsers do not properly validate input under specific conditions, aka 'Microsoft Browsers Tampering V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0786	N/A	9.8	An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0790	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0791	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0792	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0793	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0794	N/A	8.8	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulne...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0795	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0796	N/A	5.5	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0802	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0803	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0805	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privil...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0806	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0810	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0812	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0814	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0829	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0833	N/A	6.5	An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka 'Microsoft Edge Information Disclosure Vu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0835	N/A	6.5	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory, aka 'Microsoft Scripting Engine I...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0836	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0838	N/A	7.8	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0839	N/A	4.4	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Info...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0840	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0841	N/A	7.8	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0842	N/A	8.8	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0844	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0845	N/A	8.8	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execut...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0846	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0847	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0848	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0849	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0851	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0853	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0856	N/A	7.2	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0859	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0860	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0861	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0862	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0877	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0879	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0707	N/A	7.0	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffe...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0725	N/A	9.8	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Remote...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0727	N/A	7.8	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletio...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0733	N/A	5.3	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0734	N/A	8.1	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authe...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0758	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0820	N/A	7.5	A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings, aka '.NET Framework and .NET Core Denial ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0863	N/A	7.8	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0864	N/A	5.5	A denial of service vulnerability exists when .NET Framework improperly handles objects in heap memory, aka '.NET Framework Denial of Service Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0881	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0882	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0884	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0885	N/A	7.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0886	N/A	6.8	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0889	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0890	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0891	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0892	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0893	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0894	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0895	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0896	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0897	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0898	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0899	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0900	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0901	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0902	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0903	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0911	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0912	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0913	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0914	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0915	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0916	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0917	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0918	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0921	N/A	6.5	An spoofing vulnerability exists when Internet Explorer improperly handles URLs, aka 'Internet Explorer Spoofing Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0922	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0923	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0924	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0925	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0926	N/A	7.5	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0927	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0929	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0930	N/A	6.5	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclos...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0931	N/A	7.0	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0933	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0936	N/A	7.8	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevati...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0937	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0938	N/A	9.0	An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0940	N/A	7.5	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vul...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0942	N/A	5.5	An elevation of privilege vulnerability exists in the Unified Write Filter (UWF) feature for Windows 10 when it improperly restricts access to the reg...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0961	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0980	N/A	7.5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0981	N/A	7.5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0620	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0710	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0711	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0713	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0722	N/A	8.8	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0888	N/A	8.8	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0904	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0905	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0906	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0907	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0908	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0909	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0920	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0941	N/A	7.5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0943	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0948	N/A	5.5	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference t...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0959	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0972	N/A	6.5	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker send...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0973	N/A	7.8	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an inse...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0974	N/A	8.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0983	N/A	7.8	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0984	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0986	N/A	7.1	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0988	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0989	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0990	N/A	6.5	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0991	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0992	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0993	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0998	N/A	7.8	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1003	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1005	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1007	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1010	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1012	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1014	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1017	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1018	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1019	N/A	8.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerabil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1021	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1022	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1023	N/A	6.5	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1024	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1025	N/A	7.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1026	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1027	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1028	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1038	N/A	7.5	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1039	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an auth...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1040	N/A	5.9	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1041	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1043	N/A	6.8	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1044	N/A	7.8	A security feature bypass vulnerability exists when Windows Secure Kernel Mode fails to properly handle objects in memory.To exploit the vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1046	N/A	5.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1050	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1051	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1052	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1053	N/A	8.8	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1054	N/A	5.0	A security feature bypass vulnerability exists in Edge that allows for bypassing Mark of the Web Tagging (MOTW), aka 'Microsoft Edge Security Feature ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1055	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1064	N/A	7.8	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1065	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1069	N/A	7.8	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations, aka 'Task Scheduler Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1080	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1081	N/A	6.5	An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory, aka 'Microsoft Browser Informatio...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0785	N/A	9.8	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0811	N/A	7.5	A denial of service vulnerability exists in Windows DNS Server when it fails to properly handle DNS queries, aka 'Windows DNS Server Denial of Service...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0865	N/A	7.5	A denial of service vulnerability exists when SymCrypt improperly handles a specially crafted digital signature.An attacker could exploit the vulnerab...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0880	N/A	7.8	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0887	N/A	8.0	A remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an authenticated attacker abuses ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0966	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0975	N/A	6.3	A security feature bypass vulnerability exists when Active Directory Federation Services (ADFS) improperly updates its list of banned IP addresses. To...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1001	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1004	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1006	N/A	7.5	An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAM...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1037	N/A	7.0	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1059	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1062	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1063	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1067	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1071	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1073	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1074	N/A	5.5	An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic li...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1083	N/A	7.5	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests, aka '.NET Denial of Service Vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1085	N/A	7.8	An elevation of privilege vulnerability exists in the way that the wlansvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1086	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1087	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1088	N/A	7.8	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1089	N/A	7.8	An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1090	N/A	7.8	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrlvr.dll Elevation of Privi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1091	N/A	5.5	An information disclosure vulnerability exists when Unistore.dll fails to properly handle objects in memory, aka 'Microsoft unistore.dll Information D...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1092	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1093	N/A	5.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1094	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1095	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1096	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1097	N/A	5.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1102	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1103	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1104	N/A	7.5	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1106	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1107	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1108	N/A	6.5	An information disclosure vulnerability exists when the Windows RDP client improperly discloses the contents of its memory, aka 'Remote Desktop Protoc...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1113	N/A	8.8	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file.An attacker who successfull...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1117	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1118	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1119	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1120	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1121	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1122	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1123	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1124	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1126	N/A	5.3	A security feature bypass vulnerability exists in Active Directory Federation Services (ADFS) which could allow an attacker to bypass the extranet loc...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1127	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1128	N/A	8.8	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerabili...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1129	N/A	7.8	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1130	N/A	7.8	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0714	N/A	5.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0715	N/A	5.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0716	N/A	5.8	A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability c...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0717	N/A	5.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0718	N/A	5.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0720	N/A	8.0	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0723	N/A	5.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0965	N/A	7.6	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1030	N/A	4.3	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory. An attacker who successful...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1057	N/A	7.5	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1078	N/A	5.5	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory. An attacker who successfully ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1131	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1133	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability co...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1139	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1140	N/A	8.8	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1141	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1143	N/A	5.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who success...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1144	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1145	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1146	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully e...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1147	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully e...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1148	N/A	5.5	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who suc...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1149	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1150	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1151	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1152	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who succes...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1153	N/A	5.5	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who suc...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1155	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully e...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1156	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully e...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1157	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully e...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1158	N/A	5.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who success...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1159	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1162	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC). An attacker who successf...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1163	N/A	5.5	A security feature bypass exists when Windows incorrectly validates CAB file signatures. An attacker who successfully exploited this vulnerability cou...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1164	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1168	N/A	7.8	An elevation of privilege exists in the p2pimsvc service where an attacker who successfully exploited the vulnerability could run arbitrary code with ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1170	N/A	7.9	An elevation of privilege vulnerability exists when reparse points are created by sandboxed processes allowing sandbox escape. An attacker who success...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1171	N/A	5.6	An information disclosure vulnerability exists in SymCrypt during the OAEP decryption stage. An attacker who successfully exploited this vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1172	N/A	4.3	An information disclosure vulnerability exists in Azure Active Directory (AAD) Microsoft Account (MSA) during the login request session. An attacker w...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1173	N/A	7.0	An elevation of privilege vulnerability exists in the way that the PsmServiceExtHost.dll handles objects in memory. An attacker who successfully explo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1174	N/A	7.0	An elevation of privilege vulnerability exists in the way that the PsmServiceExtHost.dll handles objects in memory. An attacker who successfully explo...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1175	N/A	7.0	An elevation of privilege vulnerability exists in the way that the psmsrv.dll handles objects in memory. An attacker who successfully exploited the vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1176	N/A	7.0	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1177	N/A	7.0	An elevation of privilege vulnerability exists in the way that the rpcss.dll handles objects in memory. An attacker who successfully exploited the vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1178	N/A	7.0	An elevation of privilege vulnerability exists in the way that the ssdpsrv.dll handles objects in memory. An attacker who successfully exploited the v...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1179	N/A	7.0	An elevation of privilege vulnerability exists in the way that the unistore.dll handles objects in memory. An attacker who successfully exploited the ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1180	N/A	7.0	An elevation of privilege vulnerability exists in the way that the wcmsvc.dll handles objects in memory. An attacker who successfully exploited the vu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1181	N/A	9.8	A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker conne...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1182	N/A	9.8	A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker conne...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1183	N/A	8.8	This information is being revised to indicate that this CVE (CVE-2019-1183) is fully mitigated by the security updates for the vulnerability discussed...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1184	N/A	6.7	An elevation of privilege vulnerability exists when Windows Core Shell COM Server Registrar improperly handles COM calls. An attacker who successfully...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1186	N/A	7.0	An elevation of privilege vulnerability exists in the way that the wcmsvc.dll handles objects in memory. An attacker who successfully exploited the vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1187	N/A	5.5	A denial of service vulnerability exists when the XmlLite runtime (XmlLite.dll) improperly parses XML input. An attacker who successfully exploited th...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1188	N/A	7.5	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1190	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory. An attacker who successfully exploi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1192	N/A	4.3	A security feature bypass vulnerability exists when Microsoft browsers improperly handle requests of different origins. The vulnerability allows Micro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1193	N/A	6.4	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1194	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability co...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1195	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1196	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1197	N/A	4.2	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1198	N/A	6.5	An elevation of privilege exists in SyncController.dll. An attacker who successfully exploited the vulnerability could run arbitrary code with elevate...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1206	N/A	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1212	N/A	9.8	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets. An attacker who successfully ex...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1222	N/A	9.8	A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker conne...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1223	N/A	7.5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1224	N/A	7.5	An information disclosure vulnerability exists when the Windows RDP server improperly discloses the contents of its memory. An attacker who successful...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1225	N/A	7.5	An information disclosure vulnerability exists when the Windows RDP server improperly discloses the contents of its memory. An attacker who successful...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1226	N/A	9.8	A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker conne...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1227	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited th...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1125	N/A	5.6	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory. An attacker who successfully e...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1138	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1142	N/A	5.5	An elevation of privilege vulnerability exists when the .NET Framework common language runtime (CLR) allows file creation in arbitrary locations, aka ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1208	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1214	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1215	N/A	7.8	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1217	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1219	N/A	5.5	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Man...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1220	N/A	4.3	A security feature bypass vulnerability exists when Microsoft Browsers fail to validate the correct Security Zone of requests for specific URLs, aka '...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1221	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1232	N/A	7.8	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, ak...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1235	N/A	7.8	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of inp...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1236	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1237	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1240	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1241	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1242	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1243	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1244	N/A	6.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1245	N/A	6.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1246	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1247	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1248	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1249	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1250	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1251	N/A	5.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1252	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1253	N/A	7.8	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1254	N/A	5.5	An information disclosure vulnerability exists when Windows Hyper-V writes uninitialized memory to disk, aka 'Windows Hyper-V Information Disclosure V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1256	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1267	N/A	7.8	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable t...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1268	N/A	7.8	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1269	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1270	N/A	5.5	An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Micr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1271	N/A	7.8	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1272	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1273	N/A	5.4	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize certain error messages, ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1274	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1277	N/A	7.8	An elevation of privilege vulnerability exists in Windows Audio Service when a malformed parameter is processed, aka 'Windows Audio Service Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1278	N/A	7.8	An elevation of privilege vulnerability exists in the way that the unistore.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnera...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1280	N/A	7.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who s...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1282	N/A	5.5	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Com...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1285	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1286	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1287	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Netw...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1289	N/A	5.5	An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions, aka 'Wi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1290	N/A	8.8	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1291	N/A	8.8	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1292	N/A	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1293	N/A	5.5	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, a...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1294	N/A	4.6	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Fe...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1298	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1299	N/A	6.5	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1300	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1303	N/A	7.8	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1255	N/A	7.5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1367	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0608	N/A	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1060	N/A	8.8	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1166	N/A	5.9	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1230	N/A	6.8	An information disclosure vulnerability exists when the Windows Hyper-V Network Switch on a host operating system fails to properly validate input fro...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1238	N/A	6.4	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1239	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1307	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1308	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1311	N/A	7.8	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1315	N/A	7.8	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manage...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1316	N/A	7.8	An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup El...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1317	N/A	7.3	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1318	N/A	5.9	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transp...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1319	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1320	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1321	N/A	7.8	An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL), aka 'Microsof...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1322	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1323	N/A	7.8	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1325	N/A	5.5	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1326	N/A	7.5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1333	N/A	8.8	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1334	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1335	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1336	N/A	7.8	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1337	N/A	5.5	An information disclosure vulnerability exists when Windows Update Client fails to properly handle objects in memory, aka 'Windows Update Client Infor...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1339	N/A	7.8	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manage...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1340	N/A	7.8	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations.To exploit the vulne...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1341	N/A	7.8	An elevation of privilege vulnerability exists when umpo.dll of the Power Service, improperly handles a Registry Restore Key function, aka 'Windows Po...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1342	N/A	7.8	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting M...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1343	N/A	6.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1344	N/A	5.5	An information disclosure vulnerability exists in the way that the Windows Code Integrity Module handles objects in memory, aka 'Windows Code Integrit...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1345	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1346	N/A	6.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1347	N/A	6.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1356	N/A	6.5	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1357	N/A	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1358	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1359	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1365	N/A	9.9	An elevation of privilege vulnerability exists when Microsoft IIS Server fails to check the length of a buffer prior to copying memory to it.An attack...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1366	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scri...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1368	N/A	4.6	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Fe...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1371	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0712	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0719	N/A	9.1	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-0721	N/A	9.1	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1309	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1310	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged use...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1324	N/A	5.3	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles IPv6 flowlabel filled in packets, aka 'Windows TCP/IP ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1374	N/A	5.5	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1379	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1380	N/A	7.8	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1381	N/A	5.5	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows I...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1382	N/A	5.5	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1383	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1384	N/A	9.9	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerabil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1385	N/A	7.8	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in acce...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1388	N/A	7.8	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1390	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1391	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1393	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1394	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1395	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1396	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1397	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1398	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1399	N/A	6.2	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1405	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Win...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1406	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1408	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1409	N/A	5.5	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Win...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1411	N/A	6.5	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1413	N/A	4.3	A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1415	N/A	7.8	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1416	N/A	7.0	An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of P...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1417	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1418	N/A	3.3	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1419	N/A	8.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted Ope...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1420	N/A	7.8	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1422	N/A	7.8	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1424	N/A	8.1	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Featur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1426	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scrip...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1427	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scrip...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1428	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scrip...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1429	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1433	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1435	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1436	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1437	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1438	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1439	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1440	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1456	N/A	8.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted Ope...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-14678	N/A	10.0	SAS XML Mapper 9.45 has an XML External Entity (XXE) vulnerability that can be leveraged by malicious attackers in multiple ways. Examples are Local F...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1453	N/A	7.5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1465	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1466	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1467	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1468	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Win32k Graphics R...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1469	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1470	N/A	6.0	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1471	N/A	8.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1472	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1474	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1476	N/A	7.8	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1477	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Wi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1483	N/A	7.8	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1484	N/A	7.8	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1485	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1488	N/A	3.3	A security feature bypass vulnerability exists when Microsoft Defender improperly handles specific buffers, aka 'Microsoft Defender Security Feature B...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0601	N/A	8.1	A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates.An attacker could ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0605	N/A	8.8	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file.An attacker who successfull...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0606	N/A	8.8	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file.An attacker who successfull...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0607	N/A	5.5	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Compone...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0608	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0609	N/A	9.8	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target sy...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0610	N/A	9.8	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target sy...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0611	N/A	7.5	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0612	N/A	7.5	A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and s...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0613	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0614	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0615	N/A	5.5	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory,...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0616	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0617	N/A	6.0	A denial of service vulnerability exists when Microsoft Hyper-V Virtual PCI on a host server fails to properly validate input from a privileged user o...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0620	N/A	7.8	An elevation of privilege vulnerability exists when Microsoft Cryptographic Services improperly handles files, aka 'Microsoft Cryptographic Services E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0621	N/A	4.4	A security feature bypass vulnerability exists in Windows 10 when third party filters are called during a password update, aka 'Windows Security Featu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0623	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0625	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0626	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0627	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0628	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0629	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0630	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0631	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0632	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0633	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0634	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0635	N/A	7.8	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevati...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0637	N/A	6.5	An information disclosure vulnerability exists when Remote Desktop Web Access improperly handles credential information, aka 'Remote Desktop Web Acces...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0638	N/A	7.8	An elevation of privilege vulnerability exists in the way the Update Notification Manager handles files.To exploit this vulnerability, an attacker wou...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0639	N/A	5.5	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory,...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0640	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0641	N/A	7.8	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability,...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0642	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0643	N/A	5.5	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0644	N/A	7.8	An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names, aka 'Windows Elevation of Privilege...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0646	N/A	9.8	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-9510	N/A	5.3	A vulnerability in Microsoft Windows 10 1803 and Windows Server 2019 and later systems can allow authenticated RDP-connected clients to gain access to...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2019-1454	N/A	5.5	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0655	N/A	8.0	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0657	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Window...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0658	N/A	5.5	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory,...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0659	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0660	N/A	7.5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0661	N/A	6.8	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest op...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0662	N/A	8.8	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0663	N/A	4.2	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0665	N/A	8.1	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0666	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0667	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0668	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privileg...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0669	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privileg...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0670	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0671	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0672	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0673	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0674	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0675	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0676	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0677	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0678	N/A	7.8	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manage...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0679	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0680	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0681	N/A	7.5	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0682	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0683	N/A	7.8	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0685	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vul...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0686	N/A	7.8	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0689	N/A	6.7	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0691	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0698	N/A	5.5	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Di...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0701	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Cl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0703	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an at...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0704	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory.To exploit this vulnerability, an a...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0705	N/A	5.5	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit thi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0706	N/A	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Inform...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0707	N/A	7.8	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first h...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0708	N/A	7.8	A remote code execution vulnerability exists when the Windows Imaging Library improperly handles memory.To exploit this vulnerability, an attacker wou...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0710	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0711	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0712	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0713	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0714	N/A	5.5	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0715	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0717	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0719	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0720	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0721	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0722	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0723	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0724	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0725	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0726	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0727	N/A	7.8	An elevation of privilege vulnerability exists when the Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Conn...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0728	N/A	5.5	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Servi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0729	N/A	8.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who s...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0730	N/A	7.1	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0731	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0734	N/A	8.8	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Clie...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0735	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0737	N/A	7.8	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerab...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0738	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0739	N/A	7.8	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0740	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0741	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0742	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0743	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0744	N/A	5.5	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an atta...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0745	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0746	N/A	5.5	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0747	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Ser...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0748	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0749	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0750	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Device...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0752	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0753	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0754	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0755	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0756	N/A	5.5	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0757	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Priv...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0767	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0645	N/A	7.5	A tampering vulnerability exists when Microsoft IIS Server improperly handles malformed request headers, aka 'Microsoft IIS Server Tampering Vulnerabi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0684	N/A	8.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who s...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0690	N/A	9.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0763	N/A	7.8	An elevation of privilege vulnerability exists when Windows Defender Security Center handles certain objects in memory.To exploit the vulnerability, a...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0768	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0769	N/A	7.8	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0770	N/A	7.8	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0771	N/A	7.8	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0772	N/A	7.8	An elevation of privilege vulnerability exists when Windows Error Reporting improperly handles memory.To exploit this vulnerability, an attacker would...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0773	N/A	7.8	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0774	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0775	N/A	5.5	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attac...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0776	N/A	7.8	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles file operations.To exploit this vulnerabilit...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0777	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0778	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0779	N/A	5.5	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0780	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List S...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0781	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly handles objects in memory, aka 'Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0783	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly handles objects in memory, aka 'Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0785	N/A	7.1	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0787	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) improperly handles symbolic links, aka ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0788	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0791	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0793	N/A	7.8	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly handles file operations, aka 'Diagnostic...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0797	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0798	N/A	7.8	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an inse...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0799	N/A	7.8	An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0800	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0801	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0802	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0803	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0804	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0806	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0807	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0808	N/A	7.8	An elevation of privilege vulnerability exists in the way the Provisioning Runtime validates certain file operations, aka 'Provisioning Runtime Elevat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0809	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0810	N/A	7.8	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file creatio...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0811	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based)L, ak...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0812	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based)L, ak...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0813	N/A	7.5	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with infor...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0814	N/A	7.8	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0816	N/A	8.8	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0819	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Device Setup Manager improperly handles file operations, aka 'Windows Device Setup Man...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0820	N/A	5.5	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0822	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Language Pack Installer improperly handles file operations, aka 'Windows Language Pack...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0823	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0824	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0825	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0826	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0827	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0828	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0829	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0830	N/A	7.5	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Me...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0831	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0832	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0833	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0834	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0840	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0841	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0842	N/A	7.8	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0843	N/A	7.8	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0844	N/A	7.8	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connecte...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0845	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0848	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0849	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0853	N/A	6.5	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0854	N/A	7.1	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0857	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0858	N/A	7.8	An elevation of privilege vulnerability exists when the "Public Account Pictures" folder improperly handles junctions.To exploit this vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0859	N/A	5.5	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Servi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0860	N/A	7.8	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0861	N/A	7.8	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit thi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0864	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0865	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0866	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0867	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Or...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0868	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Or...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0869	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0871	N/A	5.5	An information disclosure vulnerability exists when Windows Network Connections Service fails to properly handle objects in memory, aka 'Windows Netwo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0877	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0879	N/A	5.5	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an atta...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0880	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0881	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0882	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0883	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0885	N/A	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows Graphics C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0887	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0896	N/A	7.8	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0897	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0546	N/A	7.8	Unquoted service path in Intel(R) Optane(TM) DC Persistent Memory Module Management Software before version 1.0.0.3461 may allow an authenticated user...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0687	N/A	8.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphic...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0699	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0784	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0794	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0821	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0888	N/A	7.8	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0889	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0895	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code E...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0907	N/A	7.8	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Component...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0910	N/A	8.4	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a gu...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0913	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0917	N/A	6.8	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0918	N/A	6.8	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0934	N/A	7.8	An elevation of privilege vulnerability exists when the Windows WpcDesktopMonSvc improperly manages memory.To exploit this vulnerability, an attacker ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0936	N/A	7.1	An elevation of privilege vulnerability exists when a Windows scheduled task improperly handles file redirections, aka 'Windows Scheduled Task Elevati...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0937	N/A	5.5	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0938	N/A	7.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted m...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0940	N/A	7.8	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notificat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0942	N/A	7.1	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connecte...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0944	N/A	7.8	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connecte...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0945	N/A	5.5	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0946	N/A	5.5	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0948	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0949	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0950	N/A	8.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0952	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0953	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0955	N/A	5.5	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Informatio...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0956	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0958	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0959	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0960	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0962	N/A	5.5	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0964	N/A	8.8	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remo...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0965	N/A	7.8	A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codec...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0966	N/A	8.8	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0967	N/A	8.8	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0968	N/A	7.5	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engin...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0969	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0970	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0982	N/A	5.5	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Grap...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0983	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows Eleva...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0985	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Ele...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0987	N/A	5.5	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Grap...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0988	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0992	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0993	N/A	6.5	A denial of service vulnerability exists in Windows DNS when it fails to properly handle queries, aka 'Windows DNS Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0994	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0995	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0996	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Ele...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0999	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1000	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1001	N/A	7.8	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notificat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1002	N/A	7.1	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerab...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1003	N/A	7.8	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Pr...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1004	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Compone...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1005	N/A	5.5	An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory, aka 'Microsoft Grap...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1006	N/A	7.8	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notificat...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1007	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1008	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1009	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Microsoft Store Install Service handles file operations in protected locations, aka...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1011	N/A	7.8	An elevation of privilege vulnerability exists when the Windows System Assessment Tool improperly handles file operations, aka 'Windows Elevation of P...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1014	N/A	7.8	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Wind...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1015	N/A	7.8	An elevation of privilege vulnerability exists in the way that the User-Mode Power Service (UMPS) handles objects in memory, aka 'Windows Elevation of...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1016	N/A	5.5	An information disclosure vulnerability exists when the Windows Push Notification Service improperly handles objects in memory, aka 'Windows Push Noti...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1017	N/A	7.8	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notificat...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1020	N/A	8.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted m...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1027	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privileg...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1029	N/A	7.8	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connecte...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1094	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Servi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0909	N/A	7.5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-0963	N/A	6.5	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Inform...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1010	N/A	7.8	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary location...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1021	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1028	N/A	7.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption V...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1035	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1037	N/A	7.5	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1048	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Win...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1051	N/A	7.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remot...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1054	N/A	7.8	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1055	N/A	6.1	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs, aka 'Micros...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1056	N/A	8.1	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to a...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1058	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1059	N/A	4.3	A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1060	N/A	7.5	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulner...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1061	N/A	8.8	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Rem...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1062	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1064	N/A	7.5	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1065	N/A	7.5	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory C...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1067	N/A	8.8	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1068	N/A	7.8	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability,...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1070	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Win...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1071	N/A	6.8	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access ...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1072	N/A	5.5	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosur...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1075	N/A	5.5	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1076	N/A	5.5	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1077	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1078	N/A	7.8	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To expl...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1079	N/A	7.8	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1081	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Wi...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1082	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1084	N/A	5.5	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values.An attacker w...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1086	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privil...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1087	N/A	7.8	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privileg...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1088	N/A	7.8	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elev...
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1090	N/A	7.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privil...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.20	3389, 445	Windows Server 2019 10.0.17763	CVE-2020-1092	N/A	7.5	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vu...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2019-7317	N/A	5.3	png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-15358	N/A	5.5	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transiti...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14814	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14830	N/A	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. E...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14837	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. E...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14839	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. E...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14845	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. E...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14846	N/A	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. E...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-14852	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Ea...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2020-1971	N/A	5.9	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL prov...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2146	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2154	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior. Easily ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2162	N/A	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prio...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2166	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0....
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2169	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2171	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2174	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 an...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2179	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7....
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2180	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2194	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2226	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-2356	N/A	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-35624	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 a...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21245	N/A	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21270	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21303	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.7.36 and p...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21304	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21344	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21367	N/A	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2021-22570	N/A	6.5	Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file'...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21417	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21427	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.37 and prior and 8.0....
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21444	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0....
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21451	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21454	N/A	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7....
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21460	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 5.7.37 and prior and ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21589	N/A	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.39 a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21592	N/A	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.39 a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21595	N/A	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21608	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.39 and prior an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2022-21617	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.39 an...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-21977	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. ...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-21980	N/A	7.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-22007	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-22015	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-22026	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-22028	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior a...
192.168.1.30	3306, 80	MySQL 5.7.33	CVE-2023-22084	N/A	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and ...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2007-3205	N/A	N/A	The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrit...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2013-2220	N/A	N/A	Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of servi...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2017-8923	N/A	9.8	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2017-9118	N/A	7.5	PHP 7.1.5 has an Out of bounds access in php_pcre_replace_impl via a crafted preg_replace call.
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2017-9120	N/A	9.8	PHP 7.x through 7.1.5 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other ...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21704	N/A	5.0	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server co...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21705	N/A	4.3	In PHP versions 7.3.x below 7.3.29, 7.4.x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via filter_var() function with F...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21706	N/A	5.3	In PHP versions 7.3.x below 7.3.31, 7.4.x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, ZipArchive::extractTo may be tricked ...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21703	N/A	7.8	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process ru...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21707	N/A	5.3	In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode t...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2021-21708	N/A	8.2	In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/m...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-31625	N/A	8.1	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-31626	N/A	7.5	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is all...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-31628	N/A	2.3	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinit...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-31629	N/A	6.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the v...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-37454	N/A	9.8	The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute a...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-31630	N/A	6.5	In PHP versions prior to 7.4.33, 8.0.25 and 8.1.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted ...
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2022-4900	N/A	6.2	A vulnerability was found in PHP where setting the environment variable PHP_CLI_SERVER_WORKERS to a large value leads to a heap buffer overflow.
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2024-25117	N/A	6.8	php-svg-lib is a scalable vector graphics (SVG) file parsing/rendering library. Prior to version 0.5.2, php-svg-lib fails to validate that font-family...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.30	3306, 80	PHP 7.4.16	CVE-2024-5458	N/A	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when v...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2021-30640	N/A	6.5	A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of t...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2021-33037	N/A	5.3	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some ci...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2021-42340	N/A	7.5	The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2022-23181	N/A	7.0	The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2022-29885	N/A	7.5	The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor inc...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2022-34305	N/A	6.1	In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples ...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2021-43980	N/A	3.7	The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (b...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2022-42252	N/A	7.5	If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via se...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2022-45143	N/A	7.5	The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In ...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-28708	N/A	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, sess...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-41080	N/A	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from ...

IP	Порты	Сервис	CVE ID	Крит.	CVSS	Описание
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-44487	N/A	7.5	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-42795	N/A	5.3	Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10....
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-45648	N/A	5.3	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 throu...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2023-46589	N/A	7.5	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 throu...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2024-38286	N/A	8.6	Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-...
192.168.1.40	8080, 8443	Tomcat 9.0.45	CVE-2025-24813	N/A	9.8	Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded...

РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ

CVE ID	IP	Рекомендации
CVE-2019-14678	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1365	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1384	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-1908	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-3711	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-42013	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-44790	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-1292	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-2068	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-22720	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-23943	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31813	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-25690	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-38408	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-38474	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-38476	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8476	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8540	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8626	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0626	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0697	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0698	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0725	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0726	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0785	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0786	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1181	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1182	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1212	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1222	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1226	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0609	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0610	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0646	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0690	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2017-8923	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2017-9120	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-37454	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2025-24813	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2022-22721	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-28615	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-38475	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0719	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0721	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-36760	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0938	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8256	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8494	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8544	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8582	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8634	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0541	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0552	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0566	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0613	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0618	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0630	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0633	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0662	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0722	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0756	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0765	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0772	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0790	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0791	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0792	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0793	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0794	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0795	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0842	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0845	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0853	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0888	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0902	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0903	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0904	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0905	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0906	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0907	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0908	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0909	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0974	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1053	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1060	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1102	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1113	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1117	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1118	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1119	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1120	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1121	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1122	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1123	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1124	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1127	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1128	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1140	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1144	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1145	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1149	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1150	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1151	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1152	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1183	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1290	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1291	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1333	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1419	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1456	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1468	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0605	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0606	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0662	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0684	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0687	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0729	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0734	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0738	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0801	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0807	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0809	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0816	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0869	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0881	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0883	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0948	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0949	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0950	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0964	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0966	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0967	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1020	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1061	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1067	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-38286	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1019	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8489	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8490	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0550	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0551	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0620	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1397	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1398	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0910	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-44224	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1471	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-21708	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2006-5051	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-6387	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0649	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0734	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1424	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0601	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0665	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1056	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31625	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0720	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0887	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0655	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1170	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-10012	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-15778	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-4807	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8411	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8413	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8415	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8423	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8432	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8453	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8471	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8484	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8485	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8497	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8550	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8554	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8561	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8562	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8584	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8599	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2018-8611	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8639	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8641	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0538	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0543	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0555	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0570	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0571	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0572	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0573	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0574	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0575	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0576	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0577	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0578	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0579	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0580	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0581	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0582	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0583	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0584	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0595	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0596	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0597	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0598	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0599	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0617	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0625	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0627	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0631	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0632	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0682	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0685	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0689	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0692	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0693	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0694	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0696	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0727	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0730	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0731	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0732	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0735	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0766	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0797	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0803	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0805	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0836	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0838	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0841	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0846	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0847	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0851	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0859	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0863	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0877	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0879	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0880	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0881	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0885	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0889	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0890	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0891	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0892	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0893	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0894	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0895	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0896	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0897	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0898	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0899	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0900	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0901	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0936	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0943	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0959	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0973	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0983	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0984	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0998	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1007	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1014	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1017	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1018	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1021	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1022	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1026	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1027	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1028	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1041	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1044	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1064	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1065	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1067	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1069	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1085	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1086	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1087	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1088	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1089	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1090	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1129	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1130	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1146	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1147	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1155	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1156	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1157	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1159	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1162	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1164	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1168	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1190	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1214	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1215	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1232	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1235	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1240	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1241	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1242	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1243	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1246	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1247	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1248	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1249	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1250	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1253	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1256	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1267	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1268	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1269	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1271	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1272	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1277	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1278	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1280	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1285	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1287	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1303	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1311	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1315	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1316	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1319	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1320	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1321	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1322	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1323	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1336	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1339	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1340	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1341	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1342	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1358	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1359	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1379	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1380	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1383	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1385	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1388	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1393	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1394	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1395	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1396	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1405	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1406	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1408	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1415	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1417	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1420	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1422	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1433	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1435	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1437	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1438	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1476	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1477	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1483	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1484	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0546	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0613	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0614	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0620	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0623	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0625	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0626	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0627	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0628	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0629	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0630	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0631	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0632	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0633	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0634	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0635	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0638	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0641	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0642	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0644	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0657	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0659	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0666	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0667	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0668	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0669	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0670	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0671	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0672	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0678	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0679	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0680	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0682	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0683	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0685	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0686	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0691	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0701	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0703	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0704	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0707	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0708	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0715	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0719	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0720	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0721	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0722	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0723	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0724	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0725	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0726	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0727	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0731	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0735	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0737	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0739	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0740	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0741	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0742	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0743	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0745	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0747	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0749	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0750	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0752	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0753	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0754	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0757	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0763	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0769	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0770	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0771	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0772	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0773	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0776	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0777	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0778	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0780	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0781	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0783	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0784	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0787	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0788	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0791	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0793	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0797	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0798	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0799	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0800	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0802	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0803	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0804	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0806	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0808	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0810	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0814	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0819	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0822	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0834	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0840	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0841	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0842	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0843	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0844	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0845	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0849	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0857	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0858	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0860	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0861	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0864	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0865	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0866	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0867	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0868	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0877	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0887	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0888	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0889	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0896	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0897	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0907	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0913	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0934	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0938	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0940	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0944	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0953	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0956	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0958	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0959	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0960	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0965	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0983	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0985	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0988	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0992	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0994	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0995	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0996	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0999	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1000	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-1001	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1003	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1004	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1006	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1008	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1009	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1010	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1011	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1014	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1015	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1017	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1021	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1027	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1028	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1029	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1048	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1051	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1054	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1068	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1070	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-1077	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1078	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1079	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1081	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1082	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1086	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1087	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1088	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1090	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1094	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-21703	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0965	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2006-20001	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-10708	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0190	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-23840	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-41524	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-41773	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-0778	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-22719	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2022-26377	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-29404	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-30556	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-4450	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-0215	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-0464	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-27522	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-31122	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-27316	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-38477	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-40898	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-17612	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8460	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8473	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8491	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8503	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8505	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8510	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8511	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8513	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2018-8517	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8541	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8542	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8543	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8551	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8552	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8555	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8556	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8557	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8583	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8588	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8617	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8618	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8619	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8624	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8625	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8629	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8631	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8643	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8653	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0539	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0545	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0565	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0567	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0568	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0590	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0591	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0592	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0593	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0603	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0605	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0606	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0607	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0609	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0610	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0611	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0634	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0637	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0639	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0640	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0642	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0644	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0645	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0650	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0651	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0652	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0655	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0665	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0666	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0667	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0680	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0688	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0739	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0752	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0753	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0763	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0769	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0771	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0773	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0780	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0783	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0784	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0806	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0810	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0811	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0812	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0820	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0829	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0860	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0861	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0862	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0865	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0884	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0911	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0912	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0913	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0914	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0915	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0916	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0917	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0918	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0920	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0922	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0923	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0924	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0925	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0926	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0927	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0929	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0933	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0937	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0940	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0941	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0980	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0981	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0988	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0989	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0991	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0992	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0993	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1001	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1003	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1004	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1005	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1006	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1024	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1025	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1038	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1051	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1052	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1055	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1057	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1059	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1062	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1063	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1080	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1083	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1092	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1103	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1104	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1106	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1107	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1133	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1138	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1188	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1194	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1206	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1208	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1217	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1221	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1223	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1224	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1225	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1236	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1237	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1239	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1255	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1298	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1300	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1307	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1308	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1326	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1335	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1366	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1367	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1371	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1390	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1426	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1427	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1428	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1429	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1453	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1485	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0611	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0612	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0640	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0645	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0660	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0673	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0674	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0681	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0710	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0711	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0712	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0713	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0767	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0768	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0811	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0812	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0813	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0823	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0824	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0825	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0826	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0827	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0828	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0829	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0830	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0831	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0832	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0833	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0848	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0895	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0909	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0968	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0969	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0970	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1035	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1037	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1058	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1060	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1062	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1064	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1065	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1092	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2017-9118	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31626	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-42340	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-29885	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-42252	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2022-45143	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-44487	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-46589	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1543	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-3712	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-0286	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-10009	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1317	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0856	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0986	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0730	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0785	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0854	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0936	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0942	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1002	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-21980	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-10010	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-51767	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8333	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0656	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0659	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0707	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0931	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1037	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1173	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1174	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1175	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1176	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1177	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1178	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1179	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1180	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1186	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1416	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-23181	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-6109	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-6110	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0678	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0690	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0695	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0701	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0710	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0711	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0712	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0713	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0886	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0966	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1043	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1230	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1309	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1310	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0661	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0917	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0918	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1071	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-25117	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1184	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0689	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-2650	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2023-51385	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8595	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8596	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0602	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0614	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0615	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0616	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0619	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0658	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0660	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0676	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0703	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0704	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0746	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0758	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0761	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0764	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0774	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0802	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0821	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0833	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0835	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0849	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0882	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0921	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0930	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0961	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0972	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0990	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1010	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1012	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1023	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1050	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1081	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1094	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1095	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1108	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1198	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1244	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1245	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1252	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1286	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1299	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1343	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1346	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1347	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1356	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1411	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1439	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1465	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1466	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1467	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0637	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0774	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0853	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0880	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0882	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0952	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0963	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0993	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-14830	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14846	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-22570	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21454	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31629	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31630	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-30640	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8592	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1193	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1238	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0975	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0635	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1399	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-4900	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1055	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-34305	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-41080	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1470	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0617	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-0734	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2018-0735	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-6111	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1971	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-23841	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-3449	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-4160	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-4304	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-45802	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-48795	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0641	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0657	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1040	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1166	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1318	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1971	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2356	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0714	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0715	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0716	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0717	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0718	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0723	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1125	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1171	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-10011	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-0727	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-3900	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8330	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8407	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8454	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8472	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8477	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8486	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8506	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8514	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8549	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8612	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8637	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8638	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8649	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0536	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0549	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0553	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0554	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0569	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0621	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0628	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0636	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0702	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0754	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0755	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0759	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0767	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0776	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0782	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0796	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0814	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0840	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0844	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0848	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-0864	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0942	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0948	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1039	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1046	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1071	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1073	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1074	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1078	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1091	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1093	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1096	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1097	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1142	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1143	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1148	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1153	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1158	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1163	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1187	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1219	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1227	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1251	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1254	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1270	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1274	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1282	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1289	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1293	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1325	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1334	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1337	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1344	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1345	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1374	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1381	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1382	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1391	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1409	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1436	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1440	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1454	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1469	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1472	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1474	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0607	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0608	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0615	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0616	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0639	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0643	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0658	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0675	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0676	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0677	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0698	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0699	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0705	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0714	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0717	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0728	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0744	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0746	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0748	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0755	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0756	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0775	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0779	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0794	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0820	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0821	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0859	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0871	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0879	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0937	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0945	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0946	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0955	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0962	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0982	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2020-0987	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1005	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1007	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1016	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1072	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1075	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1076	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1084	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-15358	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21367	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8547	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1273	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2016-20012	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2017-15906	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-15473	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-20685	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1549	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1551	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-2097	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-28330	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2022-28614	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-37436	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-0465	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-0466	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-5678	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8417	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8492	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0612	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0733	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1126	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1324	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-9510	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-7317	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-21706	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-21707	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2024-5458	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-33037	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-42795	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-45648	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1054	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2021-21704	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2014-2532	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1292	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14814	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14837	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14839	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14845	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-14852	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2146	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2154	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2166	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2169	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2179	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2180	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2194	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2226	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-35624	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21270	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21303	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21304	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2022-21344	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21417	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21427	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21608	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21617	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-21977	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-22007	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-22015	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-22026	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-22028	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-22084	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1547	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0600	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0601	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0775	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8566	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1294	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1368	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0839	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0621	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2021-2171	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2174	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21444	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21451	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21460	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21595	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8320	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8545	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8564	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0608	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0643	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0648	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0654	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0762	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-0768	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1030	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1172	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1192	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1220	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1357	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1413	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0706	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0885	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-1059	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-2162	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-21705	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21245	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21589	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-21592	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2023-28708	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1131	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1139	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1141	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1195	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1196	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1197	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2020-0663	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1563	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-36368	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2021-43980	192.168.1.40	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2019-1552	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1418	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2019-1488	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8481	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2018-8482	192.168.1.20	• Обновите до последней версии • Примените патчи безопасности
CVE-2022-31628	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2000-0143	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2001-0529	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2001-0816	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2001-0872	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2001-1380	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2001-1382	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2003-0190	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2003-0682	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2003-0693	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2003-0695	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2004-1653	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2006-5794	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2007-2768	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2007-4723	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2007-4752	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2008-3259	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2008-3844	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2008-4109	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-0796	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-1390	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-2299	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-3765	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-3766	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2009-3767	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2010-4478	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2010-4755	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2010-5107	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2011-1176	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2011-2688	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2011-4327	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2011-5000	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2012-0814	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2012-3526	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2012-4001	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности

CVE ID	IP	Рекомендации
CVE-2012-4360	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-0941	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-0942	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-2765	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-4365	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2014-1692	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2014-2653	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2014-9278	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2015-5352	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2015-5600	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2015-6563	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2015-6564	192.168.1.10	• Обновите до последней версии • Примените патчи безопасности
CVE-2007-3205	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности
CVE-2013-2220	192.168.1.30	• Обновите до последней версии • Примените патчи безопасности

ВЫВОДЫ

Обнаруженные уязвимости представляют значительные риски для безопасности сети. Игнорирование рекомендаций по их устранению может привести к серьезным последствиям, включая:

Критические и высокие уязвимости отсутствуют. Однако игнорирование низких и средних уязвимостей может привести к накоплению рисков, которые в будущем могут быть использованы для атак.