CERT.be

Vulnerability Report

TLP: White

The
Federal Cyber
Emergency Team

Contents

1 INTRODUCTION

This document provides a combined overview and assessment of several vulnerability reports and should help prioritise actions.

For each vulnerability report, this document provides the description and assessments.

Vulnerabilities are assessed as either having Low, Medium or High rating and contain where possible guidelines for action and an urgency score.

The assessment results provided in this document need to be correlated with the criticality of actual assets and possible countermeasures that are already in place.

- “**Immediate Action**” means that it is advisable to take actions asap to resolve the vulnerability or take countermeasures.
- “**To Plan**” means that we recommend actions in a planned and change management process controlled manner.
- “**To Assess**” means that the system owner needs to take the decision based on their risk appetite and the specific vulnerable assets.

2 OVERVIEW OF SCANNING PROJECTS

The table below provides an overview of all scanning reports and their risk rating.

Report Name	Risk	
SSL POODLE Scan	Low	7
HTTP Scan	Medium	8
FTP Scan	Medium	9
RDP	**High**	10
mDNS	Low	11
SNMP	Medium	12
AFP	Medium	13
NTP	Low	14
Telnet	Low	15
SSL Freak	Low	16
Port Mapper	Medium	17
VNC	Medium	18
DNS	Medium	19
Netbios	Low	20
SSDP	Medium	21
ISAKMP	Medium	22
TFTP	Low	23
RSYNC	Medium	24
SMB	**High**	25
CWMP	**High**	26
MSSQL	Medium	27
LDAP TCP	Medium	28
IPMI	**High**	29
Ubiquiti	Medium	30
Cisco Smart Install	**High**	31
NTP Monitor	Low	32
NAT-PMP	Low	33
QOTD	Low	34
CHARGEN	Medium	35
MongoDB	**High**	36

2.1 SSL POODLE Scan

Criticality	Low	Overall Risk	Low
Probability	Low	Advised Action	To Assess
Severity	Low		

Description

Hosts that allow the use of SSL v3.0 with cipher-block chaining (CBC) mode ciphers, which are vulnerable to the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack.

Assessment

The entries in this report are hosts that have the HTTPS service open towards the internet with a vulnerable cipher suite. The ciphers used are SSLv3 with cipher-block chaining (CBC) enabled. A Man in the Middle attack could be performed, which would result in decryption of the encrypted traffic, by an attacker. The first mention of this attack dates back to 2014. All major browsers have mitigation for this MitM downgrade attack since 2015 at latest.

The likelihood is rated low. An attack still requires for an attacker to be able to position himself between the client and web server.

The impact is low. As even with the vulnerable cipher suite, it is still not easy to decrypt live traffic. If an attacker is able to do this successfully, there is a possibility of information leakage, and changes to the intercepted data.

Recommendations

- In the case of vulnerable TLS implementations: Implement the updates which are available.
- Configure servers and clients to not support SSLv3 and vulnerable TLS implementations.

References

- Shadow Server – SSL POODLE Report
  https://www.shadowserver.org/what-we-do/network-reporting/ssl-poodle-report/
- Shadow Server – SSLv3 (POODLE) scanning project
  https://poodlescan.shadowserver.org/
- US Cert – SSL 3.0 Protocol Vulnerability and POODLE Attack
  https://www.us-cert.gov/ncas/alerts/TA14-290A

2.2 HTTP Scan

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the Hypertext Transfer Protocol (HTTP) running on some port and are accessible on the Internet.

Assessment

The entries in this report are hosts that have a HTTP service open towards the internet on a non-standard port. The example report shows only port TCP/8080, so the assumption is these scans only happen on port 8080. HTTP is an unencrypted protocol by default.

If it can be identified, this report also lists the type of webserver and its version, as well as any cookies it tries to set on the client.

Scans for HTTP servers are common, and port TCP/8080 is in the top 20 of most scanned ports. With banner grabbing, the vulnerabilities of a HTTP server are quickly identified. Additionally, there are free vulnerability scanning tools (like Nessus) which will show an attacker the vulnerabilities associated with the HTTP server version in one go. However, since not every HTTP server will have vulnerabilities, the likelihood of an attacker identifying and exploiting these is considered low.

The impact of such an exploitation depends on the nature of the vulnerability (and thus the version of the HTTP server). This ranges from unauthorized file access to Remote Code Execution. We would rate this as medium.

Recommendations

- Make sure the HTTP service is supposed to be online. If it is not, either close the port on the machine, or change the configuration of your firewall/reverse proxy, so as not to open the port to the internet.
- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

– Shadow Server – Open HTTP Report
https://www.shadowserver.org/what-we-do/network-reporting/open-http-report/

2.3 FTP Scan

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Low		

Description

This report identifies hosts that have an FTP instance running on port 21/TCP that's accessible on the Internet.

FTP provides no encryption (unless FTPS is utilized) and may expose sensitive information or system credentials.

If we are able to successfully negotiate a TLS or SSL connection by using an "AUTHTLS" or "AUTHSSL" command, the parsed contents of the SSL handshake and SSL certificate will be shown.

If we are not able to negotiate an FTPS connection, the "auth_tls_response" and "auth_ssl_response" fields will contain the error that returned, and the contents of the SSL-related fields will be empty.

Assessment

The entries in this report are hosts that have an FTP service open towards the internet. FTP is an unencrypted protocol by default, but some FTP servers will upgrade the connection to SSL/TLS when requested by the client.

The report shows each servers response to this SSL/TLS upgrade request and also includes encryption parameters where available. Additionally, the report shows the version of the FTP service, which could identify known vulnerabilities.

Scans for FTP servers are common, and with banner grabbing, the vulnerabilities of an FTP server are quickly identified. Additionally, there are free vulnerability scanning tools (like Nessus) which will show the attacker the vulnerabilities associated with the FTP server version in one go. However, since not every FTP server will have vulnerabilities, the likelihood of an attacker identifying and exploiting these is considered medium.

The impact of such an exploitation depends on the nature of the vulnerability (and thus the version of the FTP server). This ranges from unauthorized file up/downloads to Remote Code Execution. We would rate this as Low.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

- Shadow Server – Accessible FTP Report
  https://www.shadowserver.org/what-we-do/network-reporting/accessible-ftp-report/

2.4 RDP

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have Remote Desktop (RDP) Service running and are accessible to the world on the Internet.

Misconfigured RDP can allow miscreants access to the desktop of a vulnerable host and can also allow for information-gathering on a target host, as the SSL certificate used by RDP often contains the system's trivial hostname.

Assessment

The entries in this report are hosts that have the Remote Desktop Protocol (RDP) Service open towards the internet. The hostname and certificate presented by this service equal information leakage, and possible identification of the owner of the server. Additionally, there are known vulnerabilities on this protocol (BlueKeep and others), and it is generally considered best security practices to not have your RDP services exposed to the internet.

The likelihood of discovery is high. RDP is a high value target, and attackers are actively looking for targets.

The impact is high. Out of the many exposed RDP ports a part of them will be vulnerable. The Shadow Server reports also highlight the servers vulnerable for BlueKeep.

Recommendations

- If possible, restrict access to RDP servers to internal networks.
- If remote access is necessary use a VPN, lock accounts after multiple failed login attempts, enforce strong passwords, and use multi factor authentication wherever possible.
- Make sure the server is always up-to-date.

References

- Shadow Server – Accessible RDP Report
  https://www.shadowserver.org/what-we-do/network-reporting/accessible-rdp-report/
- Shadow Server – RDP Scanning Project
  https://rdpscan.shadowserver.org/
- Microsoft - CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- Wikipedia – Bluekeep
  https://en.wikipedia.org/wiki/BlueKeep

2.5 mDNS

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have the mDNS service running and accessible from the Internet.

Our initial probe tests to see if mDNS is accessible on the Internet and collects the information that it discloses, including a list of services that may be accessible via further mDNS probes. If a host is found to have the services "_workstation._tcp.local" or "_http._tcp.local" running, secondary probes are performed to collect whatever system information is returned. Some of the information that may be returned includes: trivial name of the device, IPv4 and IPv6 address(es) of the device (this may include RFC1918 addresses that are not meant to be leaked), MAC address information of the device, and potentially other information.

Assessment

The entries in this report are hosts that have the Multicast DNS service open towards the internet. This service leaks some information, like internal IP addresses, hostnames or MAC addresses. Products like Google Chromecast and Apple TV typically use this service for local network discovery.

A simple scanner can identify an exposed mDNS service, but the benefit for an attacker is limited. Therefore, the likelihood is set to medium.

Because there is only some minor information leakage through mDNS, the impact is set to low.

Recommendations

- Restrict access to internal networks. If the need arises to route mDNS' service over the public Internet you are using the wrong tool and switch to "real" DNS instead.

References

- Shadow Server - Open mDNS Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-mdns-report/
- Shadow Server - mDNS Scanning Project
  https://mdns.shadowserver.org/
- Wikipedia - Multicast DNS
  https://en.wikipedia.org/wiki/Multicast_DNS

2.6 SNMP

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts with SNMPv2 publicly accessible, that are responding to the community “public”, and that have the potential to be used in amplification attacks by criminals who wish to perform denial of service attacks.

Assessment

The entries in this report are hosts that have the SNMP service open towards the internet. Additionally the SNMP service is running SNMPv2, and responds to the default community string “public”. This will lead to information leakage and DOS amplification attacks.

The likelihood is rated medium.

The impact is medium, as it will lead to information leakage as well as it will enable DoS amplification attacks.

Recommendations

- Make sure SNMP is configured according to current best practices.
- Restrict access to internal networks.
- If remote access is necessary use a VPN.

References

– Shadow Server - Open SNMP Report
https://www.shadowserver.org/what-we-do/network-reporting/open-snmp-report/

– Shadow Server - SNMP scanning project
https://snmpscan.shadowserver.org/

– Helpsystems - SNMP community strings
https://community.helpsystems.com/knowledge-base/intermapper/snmp/snmp-community-strings/

2.7 AFP

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the Apple Filing Protocol (AFP) running and accessible on the Internet.

Assessment

The entries in this report are hosts that have the AFP service open towards the internet. Service version and authentication methods details are available in the report. With the right filter, you can obtain servers that allow for guest file access.

The likelihood is considered medium because this can be a very easy target which does not even require an exploit.

The impact is set to medium as can be accessed by a malicious party.

The overall risk is set to medium.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary use a VPN.

References

- Shadow Server – Accessible AFP Report https://www.shadowserver.org/what-we-do/network-reporting/accessible-afp-report/

2.8 NTP

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Description

This report identifies NTP servers that have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

The NTP version command is a Mode 6 query for READVAR. While not as bad as the Mode 7 query for MONLIST, the queries for READVAR will normally provide around 30x amplification.

Assessment

The entries in this report are hosts that have the NTP Service open towards the internet and are listening to version queries. This service can be used by attackers in a DoS amplification attack.

The likelihood is set to medium, as it requires no authentication to abuse.

Because the DoS amplification is relatively small, the impact is set to low.

Recommendations

- Restrict access to internal networks or VPNs if possible.
- If access from the public Internet is desired, make sure to use a safe configuration.[3][4]

References

– Shadow Server - NTP Version Report
https://www.shadowserver.org/what-we-do/network-reporting/ntp-version-report/

– Shadow Server - NTP Scanning Project
https://scan.shadowserver.org/ntpversion/

– [3]: Cymru NTP template

https://www.team-cymru.com/secure-ntp-template.html

– [4]: NTP configuration

http://support.ntp.org/bin/view/Support/AccessRestrictions

2.9 Telnet

Criticality	Low	Overall Risk	Low
Probability	Low	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have a Telnet instance running on port 23/TCP that are accessible on the Internet.

Telnet provides no encryption and may expose sensitive information or system credentials.

Assessment

The entries in this report are hosts that have the telnet service open towards the internet. Telnet is a communication protocol that does not encrypt anything. This means credentials (for authentication) or information can leak to an attacker who is able to intercept the traffic.

The likelihood is rated low. An attack still requires for an attacker to be able to position him or herself between the client and the telnet server.

The impact is considered low. Besides a possible information leak there are no other abuse options.

Recommendations

- If possible disable telnet altogether and switch to modern, encrypted protocols like SSH.
- Restrict access to the service to internal networks.
- If remote access is absolutely necessary, use a VPN through which only authorized personell can access the devices.

References

- Shadow Server – Accessible Telnet Report
  https://www.shadowserver.org/what-we-do/network-reporting/accessible-telnet-report/
- Shadow Server – Telnet scanning project
  https://scan.shadowserver.org/telnet/
- Wikipedia – Telnet
  https://en.wikipedia.org/wiki/Telnet

2.10 SSL Freak

Criticality	Low	Overall Risk	Low
Probability	Low	Advised Action	To Assess
Severity	Medium		

Description

This report identifies hosts that allow the use of SSL/TLS with RSA_EXPORT ciphers (aka “export-grade” encryption).

Hosts with these weakened ciphers can be used in a man-in-the-middle attack, which forces a browser to use a weak export key, which is easily crackable. This is called a FREAK (Factoring RSA Export Keys) attack.

Assessment

The entries in this report are hosts that have the HTTPS service open towards the internet with a vulnerable cipher suite. The ciphers used are “export grade” which translates to “weakened on purpose”. A Man in the Middle attack could be performed easily, which would result in decryption of the (weakly) encrypted traffic by an attacker. The first mention of this attack dates back to 2015. All major OS’s and browsers have mitigated this MitM attack vector since 2015.

The likelihood is rated low. An attack still requires for an attacker to be able to position himself between the client and web server and has to be able to downgrade the cipher suite, which is no longer possible with mainstream OS/browsers.

The impact is medium. As there is a possibility of information leakage, and changes to the intercepted data.

Recommendations

- For all vulnerable clients updates are available since 2015.[1]
- Disable the RSA_EXPORT ciphers on your server to make it impossible for clients to even try using them in communicating with you. A MITM attack would simply fail as the server refuses connections that try to use these ciphers.

References

- Shadow Server - SSL FREAK Report
  https://www.shadowserver.org/what-we-do/network-reporting/ssl-freak-report/
- Shadow Server - SSL Export Ciphers (FREAK) scanning project
  https://freakscan.shadowserver.org/
- MiTLS - Freak
  https://mitls.org/pages/attacks/SMACK#freak

2.11 Port Mapper

Criticality	Medium	Overall Risk	Medium
Probability	High	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the Portmapper service running and accessible on the public Internet.

This service has the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

In addition to being used in denial of service attacks, portmapper can be used to obtain a large amount of information about the target, including the NFS exports that are hosted by that device, if the mountd program is also accessible.

Assessment

The entries in this report are hosts that have the Portmapper Service open towards the internet. This service can leak information and can also be used by attackers in DoS amplification attacks. The portmapper service is one you will encounter often, but it takes manual verification to further analyze its vulnerability to the above issues. A lot of the results from the report will be false positives.

The likelihood is high. The report will show that Portmapper is often exposed to the internet, however, there tend to be a lot of false positives for this vulnerability.

The impact is high, as there is both information leakage and DoS amplification attacks possible.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

- Shadow Server - Open Portmapper Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-portmapper-report/
- Shadow Server - Portmapper Scanning Project
  https://portmapperscan.shadowserver.org/
- Virgin Media - Similar Shadow Server effort in the UK
  https://www.virginmedia.com/help/open-portmapper-vulnerability
- Wikipedia - Portmapper service
  https://en.wikipedia.org/wiki/Portmap
- US CERT - Alert (TA14-017A)
  https://www.us-cert.gov/ncas/alerts/TA14-017A
- Level3 - Portmapper blog post
  http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

2.12 VNC

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have a VNC instance running on port 5900/TCP that are accessible on the Internet.

If improperly configured, VNC may allow remote access to a desktop in an unintended manner.

Assessment

The entries in this report are hosts that have the VNC service open towards the internet. VNC is a Remote Administration Tool (RAT) which is used to take over the desktop of the system that has the service running. The VNC service has an option to authenticate the user with a password, but it is not mandatory. The Shadow Server report does not include whether a password has been set, so further verification is required.

The likelihood is rated medium. This is typically something script kiddies will be looking/scanning for.

The impact is considered medium. If successful, the system is completely taken over by the attacker. However, most systems will have a password set, in which case there are little known vulnerabilities.

Recommendations

- If possible, restrict access to VNC servers to internal networks.
- If remote access is necessary use a VPN, lock accounts after multiple failed login attempts, enforce strong passwords, and use multi factor authentication wherever possible.

References

- Shadow Server – Accessible VNC Report
  https://www.shadowserver.org/what-we-do/network-reporting/accessible-vnc-report/
- Shadow Server – VNC scanning project
  https://vncscan.shadowserver.org/

2.13 DNS

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies DNS servers that have the potential to be used in DNS amplification attacks by criminals that wish to perform denial of service attacks.

Assessment

The entries in this report are hosts that have a DNS open-resolver service open towards the internet. DNS Open-resolvers are DNS servers responding to recursive queries for arbitrary domain names from anywhere on the Internet. They can be used in DoS amplification attacks.

The likelihood is medium because the service is running on a well-known port.

The impact is set to medium as exploiting this service can result in it being used for DoS amplification attacks.

The overall risk is set to medium.

Recommendations

- Make sure your DNS resolver handles only queries from certain (i.e. your) clients.
- Use source-IP verification to make address spoofing impossible/much harder.
- Use Response Rate Limiting, i.e. limit the number of queries a client is allowed to make per second.
- Disable recursive queries on authoritative name servers all together.

References

- Shadow Server – DNS Open Resolvers Report
https://www.shadowserver.org/what-we-do/network-reporting/dns-open-resolvers-report/

- Shadow Server – DNS Scanning Project
https://dnsscan.shadowserver.org/

- CERT Germany – DNS Open Resolver
https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/CERT-Reports/HOWTOs/DNS-Open-Resolver/DNS-Open-Resolver_node.html

2.14 Netbios

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have the NetBIOS service running and accessible on the Internet.

These services have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

Assessment

The entries in this report are hosts that have the NETBIOS Service open towards the internet. This service will leak hostname and domain information of the host running it. It can also be used by attackers in a DoS amplification attack.

The likelihood is set to medium, as it requires no authentication to abuse.

Because both the information leakage and the DoS amplification are small, the impact is set to low.

Recommendations

- Disable NetBIOS if you don't absolutely need it.
- Restrict access to NetBIOS to internal networks.

References

- Shadow Server - Open NETBIOS Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-netbios-report/
- Shadow Server - NETBIOS Scanning Project
  https://scan.shadowserver.org/netbios/

2.15 SSDP

Criticality	Medium	Overall Risk	Medium
Probability	Low	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the Simple Service Discovery Protocol (SSDP) running and accessible on the Internet.

These services have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

Assessment

The entries in this report are hosts that have the SSDP service open towards the internet. This service can be used in DoS amplification attacks.

The likelihood is rated low.

The impact is medium, as there is only a medium leverage DoS amplification attack possible.

Recommendations

- Turn off SSDP. Today it is mostly used in conjunction with UPnP which also shouldn't be reachable from the public Internet.
- If you definitely need SSDP on your network, make sure access is restricted to internal networks.

References

- Shadow Server - Open SSDP Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-ssdp-report/
- Shadow Server - SSDP scanning project
  https://ssdpscan.shadowserver.org
- Cloudflare - SSDP DDoS attack
  https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/

2.16 ISAKMP

Criticality	Medium	Overall Risk	Medium
Probability	Low	Advised Action	To Plan
Severity	High		

Description

This report identifies hosts that have a vulnerable IKE service accessible on the Internet.

Assessment

The entries in this report are hosts that run a vulnerable version of ISAKMP.

A vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information.

There are a couple of CVE entries associated with this vulnerability. You can find more details in the references section below.

The likelihood is low, as a Man-in-the-Middle attack requires a prior network compromise.

The impact is high because the contents of the VPN tunnel can be decrypted.

Recommendations

- Roll out the update.

References

- Shadow Server - Vulnerable ISAKMP Report
  https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-isakmp-report/
- Shadow Server - ISAKMP Scanning Project
  https://isakmpscan.shadowserver.org/
- Cisco - ISAKMP Security Advisory
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1
- MITRE - CVE-2016-6415
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6415

2.17 TFTP

Criticality	Low	Overall Risk	Low
Probability	Low	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have the TFTP service running and accessible on the Internet.

Our probe tests to see if the TFTP service is accessible and will either return the file that we are asking for or return an error code. Note, we are not testing to see if file upload is enabled.

Also note that unlike other UDP services that we test for, the response from TFTP is often received on a port that is different than what was queried! Probes sent to a host on port 69/UDP may generate responses that source from ephemeral high ports.

Assessment

The entries in this report are hosts that have the TFTP service open towards the internet. TFTP is the Trivial File Transfer Protocol, which is a “dumbed down” version of the FTP protocol. It does not support authentication nor encryption.

The likelihood is rated low. An attacker would have to brute force file names before he/she could download anything. An alternate attack would be to Man in the Middle between the client and the TFTP server, after which files could also be intercepted while the client downloads them.

The impact is considered low. Besides a possible information leak there are no other abuse options.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

- Shadow Server – Open/Accessible TFTP
  https://www.shadowserver.org/what-we-do/network-reporting/open-accessible-tftp-report/
- Shadow Server – TFTP scanning project
  https://tftpscan.shadowserver.org/
- Wikipedia – TFTP
  https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

2.18 RSYNC

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Low		

Description

This report identifies hosts that have the rsync service running, bound to a network port (873/tcp) and accessible on the Internet without a password.

Assessment

The entries in this report are hosts that have the Rsync service open towards the internet, not secured with a password. Rsync is an open source incremental file transfer system. It was not possible to replicate the behavior from Shadow Server. Not a single one of the IP's in the report allows for passwordless file/directory listing.

The likelihood is rated medium. It is unclear how to replicate the Shadow Server scanning.

The impact is low, as there are no abuse scenarios here besides information leakage (download) and possible data changes (upload).

Recommendations

- If RSync is absolutely needed to send files over the internet, use a VPN or SSH Tunnel.
- If a VPN or tunnel is not possible, use a very strong password and set-up rate-limiting to somewhat mitigate brute-force attacks

References

– Shadow Server – Accessible Rsync Report
https://www.shadowserver.org/what-we-do/network-reporting/accessible-rsync-report/

– Rsync – Homepage
https://rsync.samba.org/

2.19 SMB

Criticality	High	Overall Risk	High
Probability	Medium	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have an SMB instance running on port 445/TCP that are accessible on the Internet.

This service should not be exposed to the Internet.

Assessment

The entries in this report are hosts that have the SMB service open towards the internet. The SMB service is used for Windows fileshares and has many famous vulnerabilities amongst which are Eternalblue, EternalRomance and EternalChampion.

The likelihood is rated medium. There will be many attackers and malware looking to exploit this service, but identifying vulnerable hosts requires further manual verification.

The impact is high, as it will give attackers complete control of the target system.

Recommendations

- Restrict access to internal networks, if possible.
- If remote access is necessary use a VPN, enforce strong passwords and follow best practices

References

- Shadow Server – Accessible SMB Report
  https://www.shadowserver.org/what-we-do/network-reporting/accessible-smb-report/
- Shadow Server - SMB Scanning Project
  https://smbscan.shadowserver.org/
- Wikipedia - Eternalblue
  https://en.wikipedia.org/wiki/EternalBlue

2.20 CWMP

Criticality	High	Overall Risk	High
Probability	Medium	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the CPE WAN Management Protocol (CWMP) running and accessible on the Internet.

Assessment

The entries in this report are hosts that have the CWMP service open towards the internet. If this service is poorly implemented, it can be hijacked by an attacker through man-in-the-middle attacks (e.g. DNS redirection).

The likelihood is considered medium because most CWMP implementations are not vulnerable. Manual verification is required.

The impact is set to high as exploiting this service can result in a Remote Code Execution.

Recommendations

- Block access to ACSs and CPEs from outside of your network.

References

- Shadow Server - Open CWMP Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-cwmp-report/
- Shadow Server - CWMP Scanning Project
  https://cwmpscan.shadowserver.org/
- Wikipedia - TR-069
  https://en.wikipedia.org/wiki/TR-069

2.21 MSSQL

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Low		

Description

This report identifies hosts that have the MS-SQL Server Resolution Service running and accessible on the Internet.

These services have the potential to expose information about a client’s network on which this service is accessible and the service itself can be used in UDP amplification attacks.

Assessment

The entries in this report are hosts that have the MS-SQL Server Resolution Service open towards the internet. This service has no known vulnerabilities but will leak some information by default. It can also be used for DoS amplification attacks.

The likelihood is set to medium, while the risk is set to low.

Recommendations

- Restrict access to internal networks.
- If remote acces is necessary, use a VPN.

References

- Shadow Server - Open MS-SQL Server Resolution Service Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-ms-sql-server-resolution-service-report/
- Shadow Server - MSSQL Scanning Project
  https://mssqlscan.shadowserver.org/

2.22 LDAP TCP

Criticality	Medium	Overall Risk	Medium
Probability	High	Advised Action	To Plan
Severity	Low		

Description

This report identifies hosts that have an LDAP instance running on port 389/UDP (or TCP) that are accessible on the Internet.

These hosts are often Active Directory servers. In addition to allowing for an ~60x amplification vector, the data disclosed by the server could reveal large amounts of information about the network that the server resides on.

Assessment

The entries in this report are hosts that have an LDAP service open towards the internet. As you can see in the report details, there is a large amount of information from the Active Directory domain which can be queried by an unauthenticated user. This means an LDAP server leaks information by default. Additional to that these LDAP services can also be leveraged by malicious actors in DoS amplification attacks.

Because the LDAP servers in this report are running on the default port, they are very easy to locate and analyze. This makes the likelihood high.

The LDAP servers leak the “standard” information which can be found in the report. There is a possibility for additional data leakage which requires manual verification. Add to this the DoS amplification, and the impact is low.

Recommendations

- Restrict access to the server(s) to internal networks.
- If remote access is necessary, set up a VPN which authorized people can use to access the server(s).

References

– Shadow Server - Open LDAP Report
https://www.shadowserver.org/what-we-do/network-reporting/open-ldap-report/

– Shadow Server - LDAP Scanning Project
https://scan.shadowserver.org/cldap/

– Shadow Server - Open LDAP TCP Report
https://www.shadowserver.org/what-we-do/network-reporting/open-ldap-tcp-report/

2.23 IPMI

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the Intelligent Platform Management Interface (IPMI) service open (port 623/udp) and accessible from the Internet.

IPMI is the base of most of the Out Of Band / Lights Out management suites and is implemented by the server's Baseboard Management Controller (BMC). The BMC has near complete access and control of the server's resources, including, but not limited to, memory, power, and storage. Anyone that can control your BMC (via IPMI) can control your server.

IPMI instances in general are known to contain a variety of vulnerabilities, some more serious than others. In short, you really do not want to expose IPMI to the Internet.

Assessment

The entries in this report are hosts that have an IPMI service open towards the internet. Also included are the IPMI version, and security related IPMI parameters of the host.

IPMI is a total disaster with regards to security. It can be compared to persistent malware with total server control. Opening IPMI (on the standard port) towards the internet is a very dangerous move and will certainly attract malicious attacks. An IPMI can be configured to allow anonymous logins and will almost always easily leak stored credentials. There are plenty of known exploits available for IPMI.

It being such an attractive target with weak security, the likelihood is rated as high.

Due to the nature of IPMI, the impact of a compromise is a complete server takeover, including the OS and data which runs on the server. Additionally, it is relatively easy to extract any stored credentials. Therefore, it is rated as very high.

Recommendations

- Restrict access to IPMI to your internal networks.
- If remote access from outside of your networks is necessary use a VPN through wich authorized employees can connect to IPMI.

References

- Shadow Server – Open IPMI Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-ipmi-report/
- Shadow Server – IPMI Scanning Project
  https://ipmiscan.shadowserver.org/
- Dan Farmer – IPMI Report
  http://fish2.com/ipmi/
- US-CERT - alert TA13-207A
  https://www.us-cert.gov/ncas/alerts/TA13-207A

2.24 Ubiquiti

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the Ubiquiti Discovery service running and accessible on the Internet.

These services have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks. In addition, they expose a large amount of information about the system running the service.

The service is tested by sending a UDP packet containing a four-byte payload to UDP port 10001.

Assessment

The entries in this report are hosts that have the Ubiquity Discovery service open towards the internet. The Ubiquity Discovery Service is a service which can be used by attackers in 30x DoS amplification attacks. It also leaks information about the network it is connected to.

The likelihood is rated medium. There has been plenty of activity on this port in the past years. Refer to the references for a report from Rapid7.

The impact is considered medium. Besides the information leak it can also be abused for DoS Amplification attacks.

Recommendations

- Restrict access to internal networks or VPNs if possible.
- If access from the public Internet is desired, make sure to use a safe configuration.

References

- Shadow Server – Open Ubiquity Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-ubiquiti-report/
- Rapid7 – Ubiquity Discovery Service Exposures
  https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/

2.25 Cisco Smart Install

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the Cisco Smart Install feature running and are accessible to the Internet at large.

This feature can be used to read or potentially modify a switch's configuration.

Assessment

The entries in this report provide an overview of internet facing Cisco network devices, which have the Smart Install service enabled. This service has a vulnerability which allows for an unauthenticated user to read and possibly modify the devices configuration.

The likelihood is considered high as there is a known exploit for this vulnerability, and a scanner in available in Metasploit.

The impact is set to high as it can lead to a dump of the running config, which can be followed by the password cracking of the switch credentials.

Recommendations

- Deactivate Cisco Smart Install after successful installation if possible.
- Restrict access to internal networks.
- If remote access is absolutely necessary, use a VPN.

References

– Shadow Server - Cisco Smart Install Report
https://www.shadowserver.org/what-we-do/network-reporting/accessible-cisco-smart-install-report/

– Shadow Server - Smart Install Scanner Project
https://smartinstallscan.shadowserver.org/

– Rapid7 Blog - Cisco SMI RCE
https://blog.rapid7.com/2018/03/29/cisco-smart-install-smi-remote-code-execution-what-you-need-to-know/

2.26 NTP Monitor

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Description

This report identifies NTP servers that have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

The NTP monitor command is a Mode 7 query for MON_GETLIST_1.

Assessment

The entries in this report are hosts that have the NTP Service open towards the internet and are listening to monitoring queries. This service can be used by attackers in a DoS amplification attack.

The likelihood is set to medium, as it requires no authentication to abuse.

Because the DoS amplification is relatively small, the impact is set to low.

Recommendations

- Restrict access to internal networks or VPNs if possible.
- If access from the public Internet is desired, make sure to use a safe configuration (cfr. NTP section).

References

– Shadow Server - NTP Monitor Report
https://www.shadowserver.org/what-we-do/network-reporting/ntp-monitor-report/

– Shadow Server - NTP Monitor Scanning Project
https://scan.shadowserver.org/ntpmonitor/

2.27 NAT-PMP

Criticality	Low	Overall Risk	Low
Probability	Low	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have the NAT Port Mapping Protocol (NAT-PMP) running and accessible on the Internet.

These services have the potential to expose information about a client’s network on which this service is accessible.

Assessment

The entries in this report are hosts that have the NAT-PMP Service open towards the internet. This service has no known vulnerabilities but will leak some information by default.

The likelihood is set to low, as the only known attack vector is a faulty implementation, where the NAT-PMP device will accept connections on an untrusted interface.

The impact is low, as a successful attack would only result in information leakage.

Recommendations

- Disable NAT-PMP if possible.
- Restrict access to internal networks.
- If you are using miniupnp: It's configuration may well be the origin of the problem. Thus, ensure that you have version 1.8.20141022 or later installed.

- Make sure NAT-PMP is securely configured:

1. WAN and LAN interfaces are correctly assigned.
2. NAT-PMP requests are accepted only on internal interfaces.
3. Port mappings are only opened for the requesting internal IP address.

References

- Shadow Server – Open NAT-PMP Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-nat-pmp-report/

- Shadow Server – NAT-PMP Scanning Report
  https://scan.shadowserver.org/natpmp/

2.28 QOTD

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Description

This report identifies hosts that have the Quote of the Day (QOTD) service running and accessible on the Internet.

These services have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks. The service is tested by sending a UDP packet containing a single carriage return to UDP port 17.

Assessment

The entries in this report are hosts that have the Quote of the Day (QOTD) Service open towards the internet. This service can be used by attackers in DoS amplification attacks.

The likelihood is medium. The report will show that QOTD is a service that is rarely exposed to the internet.

The impact is low, as there is only a medium leverage DoS amplification attack possible.

Recommendations

- If possible, turn off the service on 17/UDP.
- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

- Shadow Server - QOTD Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-qotd-report/
- Shadow Server - QOTD Scanning Project
  https://scan.shadowserver.org/qotd/
- Virgin Media - QOTD Report
  https://www.virginmedia.com/help/quote-of-the-day-vulnerability-alert

2.29 CHARGEN

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	Low		

Description

This report identifies hosts that have the CharGen service running and accessible on the Internet.

These services have the potential to be used in amplification attacks by malicious actors that wish to perform denial of service attacks.

The service is tested by sending a UDP packet containing a single carriage return to UDP port 19.

Assessment

The entries in this report are hosts that have the CharGen service open towards the internet. This service can be abused by malicious actors in DoS amplification attacks.

The likelihood is considered medium because it is fairly simple to include these hosts in a DoS amplification attack.

The impact is set to low as there are no other vulnerabilities known for the CharGen service.

The overall risk is set to medium.

Recommendations

- Turn off the CHARGEN-service or at least restrict access to the local network if you really need it or are not able to turn it off.

References

– Shadow Server - Open CharGen Report
https://www.shadowserver.org/what-we-do/network-reporting/open-chargen-report/

– Shadow Server - Chargen Scanning Project
https://scan.shadowserver.org/chargen/

2.30 MongoDB

Criticality	High	Overall Risk	High
Probability	Medium	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the MongoDB NoSQL database running and accessible on the Internet.

While authentication is available for MongoDB, in many instances this authentication is not enabled.

- Our initial probe tests to see if MongoDB is accessible on the Internet and collecting the system information that it discloses.
- A secondary probe is then performed to determine if a list of databases can be obtained. If an error message is generated in response to this probe, the “visible_databases” field will say “none visible”, but if no error message is generated (indicating that no authentication is in use), the “visible_databases” field will list the first five databases that were returned.

Assessment

The entries in this report are hosts that have the MongoDB service open towards the internet. This service has multiple vulnerabilities which allow an attacker to extract data from the DB. The report includes the version of MongoDB, which makes it easy to map its vulnerabilities.

Additionally, there are a lot of MongoDB services which are not secured. This means an attacker can extract data and make changes while unauthenticated. There have been hacking groups doing this on a mass scale like Unistellar.

The likelihood of an attacker abusing one of the detected MongoDB services is medium. It requires manual verification to identify vulnerabilities and to assess the configured security of the service.

If an attacker successfully breaches a MongoDB service, he/she will have read and/or write access to the database. That is why the impact is set to high.

Recommendations

- Restrict access to the database server to internal networks.
- If remote access is necessary use a VPN or at least enable authentication[2] and make sure strong passwords are used.

References

- Shadow Server – Open MongoDB Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-mongodb-report/
- Shadow Server – MongoDB Scanning Project
  https://mongodbscan.shadowserver.org/
- MongoDB – Homepage
  https://www.mongodb.com

- MITRE – MongoDB CVE
  https://www.cvedetails.com/vulnerability-list/vendor_id-12752/product_id-25450/Mongodb-Mongodb.html
- BleepingComputer – Unistellar MongoDB hack
  https://www.bleepingcomputer.com/news/security/over-12-000-mongodb-databases-deleted-by-unistellar-attackers/

3 OTHER VULNERABILTIES

3.1 Elastic Search

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have Elasticsearch running and accessible on the Internet.

On its own, Elasticsearch does not support authentication or restrict access to the datastore, so it is possible that any entity that can access the Elasticsearch instance may have complete control to do what they will with it. The probe that we are using is a “GET / HTTP/1.1” sent to port 9200/tcp.

Assessment

The entries in this report are hosts that have an Elasticsearch service open towards the internet. There are multiple ways to abuse this service. Natively it does not support authentication, so any unauthenticated attacker can abuse the service. Additionally, there are known vulnerabilities for the service. Connecting via HTTP to the service (TCP/9200) will give anyone the version of Elasticsearch, which makes it easy to identify vulnerabilities.

The likelihood is high because the service is running on a well-known port, and Elasticsearch provides useful information natively to any unauthenticated attacker.

The impact is set to high as exploiting an unpatched Elasticsearch service could result in Remote Code Execution.

The overall risk is set to high.

Recommendations

- Restrict access to the database server to internal networks.
- If remote access is necessary use a VPN or at least enable authentication[2] and make sure strong passwords are used.

References

– Shadow Server – Open Elasticsearch Report
https://www.shadowserver.org/what-we-do/network-reporting/open-elasticsearch-report/

– Shadow Server - Elasticsearch Scanning Project
https://esscan.shadowserver.org/

– CVE details – Elasticsearch
https://www.cvedetails.com/vulnerability-list/vendor_id-13554/Elasticsearch.html

3.2 Memcached key

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the Memcached key-value store running and accessible on the Internet.

Since this service does not support authentication, any entity that can access the Memcached instance can have complete control over the key-value store. In addition, instances of Memcached that are accessible via UDP may be abused in amplification-style denial of service attacks.

Assessment

The entries in this report are hosts that have the Memcached service open towards the internet. This service has a serious vulnerability if which has been patched in version 1.5.6. As you can see in the report, there are lots of hosts which expose a Memcached service older than that. This allows an attacker to perform a DoS amplification attack with an amplification factor of up to 51.000 (!).

It is fairly easy to identify this service and version, as well as performing a DoS amplification attack. Therefore, the likelihood is high.

The impact of a DoS amplification attack is rated high in this case, because of the massive amplification factor.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary use a VPN.
- Deactivate UDP on the memcached server.

References

- Shadow Server – Open Memcached Report
  https://www.shadowserver.org/what-we-do/network-reporting/open-memcached-report/
- Shadow Server – Memcached Scanning Project
  https://memcachedscan.shadowserver.org/
- Memcached – Homepage
  http://memcached.org/
- Cloudflare – Memcached DDoS Attack
  https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/

3.3 - Open Redis Key-Value Store

Criticality	Medium	Overall Risk	Medium
Probability	Medium	Advised Action	To Plan
Severity	High		

Description

This report identifies hosts that have the Redis key-value store running and accessible on the Internet.

See redis.io for more information on Redis. Since this service does not support authentication, any entity that can access the Redis instance can have complete control over the key-value store.

Assessment

The entries in this report are hosts that have the Redis Service open towards the internet. Redis is an in-memory data store which focuses on speed. There is no support for authentication, so anyone with access to the Redis service has read and write access to the entire data store.

The likelihood is rated medium.

The impact is high, there is a risk of information leakage and data changes.

Recommendations

- Restrict access to internal networks.
- If remote access is necessary, use a VPN.

References

– Shadow Server - Open Redis Report
https://www.shadowserver.org/what-we-do/network-reporting/open-redis-report/

– Shadow Server - Redis Scanning Project
https://redisscan.shadowserver.org/

– Redis - Homepage
https://redis.io/

3.4 Accessible X Display Manager Control Protocol

Criticality	Low	Overall Risk	Low
Probability	Medium	Advised Action	To Assess
Severity	Low		

Descriptions

This report identifies hosts that have the X Display Manager service running and accessible on the Internet.

Our probe tests to see if the X Display Manager is accessible by sending a “Query” packet to the XDMCP port (177/UDP) and listening for the responses.

The responses received are typically either of the “Willing” type, which means that the X Display Manager is willing to provide service, or the “Unwilling” type, which means that the X Display Manager is not willing to provide services.

XDMCP leaks information about the host system and, in addition, it can be used in an amplification attack, providing an approximate 7x amplification. Please note that it does not matter if XDMCP responds with a “Willing” or an “Unwilling”; the service provides the same level of amplification.

Assessment

The entries in this report are hosts that have the X Display Manager Control Protocol (XDMCP) service open towards the internet. The XDMCP service provides a uniform mechanism for an autonomous display to request login service from a remote host. An attacker can abuse this service because it will leak information, as well as perform a 7x DoS amplification.

The likelihood is rated medium. There are more interesting services which attackers can find and abuse.

The impact is considered low. The amplification factor is relatively low, and the information leakage is limited.

Recommendations

- If possible, restrict access to RDP servers to internal networks.
- If remote access is necessary use a VPN, lock accounts after multiple failed login attempts,[2] enforce strong passwords, and use multi factor authentication wherever possible

References

– Shadow Server – Accessible XDMCP Report
https://www.shadowserver.org/what-we-do/network-reporting/accessible-xdmcp-service-report/

– Shadow Server – XDMCP scanning project
https://xdmcpscan.shadowserver.org/

– X.org - XDMCP
https://www.x.org/releases/X11R7.6/doc/libXdmcp/xdmcp.html

3.5 - ddos_amplification

Criticality	High	Overall Risk	High
Probability	Medium	Advised Action	Immediate Action
Severity	High		

Description

This report contains observed reflected amplification DDoS events.

This category of DDoS attacks utilizes UDP-based, open, amplifiable services to reflect packets to a victim, by spoofing the source IP address of the packets sent by the amplifier to the victim’s IP address.

Depending on the protocol and type of open services abused, the size of the original packet content sent by the attacker can be amplified in the service response multiple times (even by a factor of hundreds), flooding the victim with packets and enabling DDoS.

Honeypots that emulate open and amplifiable services can be used to detect this kind of abuse. However, as the source of these attacks is spoofed to the victim address, it is possible only to report on victims being abused, not on the source of the DDoS.

This report type was enabled as part of the EU Horizon 2020 SISSDEN Project.

Assessment

The entries in this report are hosts that have been targeted by a DDoS attack. They are in no way malicious, and there is nothing identifiable on their end (service, malware, user) which could indicate this would happen, or could happen again in the future.

The likelihood of this happening again is considered medium as a DDoS is often repeated to the same target.

The impact is set to high as a DDoS attack can bring down a server or host if not behind DDoS-protection services.

The overall risk is set to high because of the potential damage to others.

References

- Shadow Server – Amplification DDoS Victim Report
  https://www.shadowserver.org/what-we-do/network-reporting/amplification-ddos-victim-report/
- EU SISSDEN
  https://sissden.eu/

3.6 - scan_adb

Criticality	High	Overall Risk	High
Probability	High	Advised Action	Immediate Action
Severity	High		

Description

This report identifies hosts that have the Android Debug Bridge (ADB) running, bound to a network port (5555/tcp) and accessible on the Internet.

Assessment

The entries in this report are hosts that have the ADB service open towards the internet. Any unauthenticated user can connect to the ADB, allowing full root access to the device or emulator.

The likelihood is considered medium. This is a very easy target which does not even require an exploit.

The impact is set to high as the device can be taken over completely by a malicious party.

The overall risk is set to high.

Recommendations

- Restrict access to internal networks.
- If remote access is absolutely necessary, use a VPN.

References

– Shadow Server – Accessible ADB Report
https://www.shadowserver.org/what-we-do/network-reporting/accessible-adb-report/

3.7 scan_db2

Criticality	Medium	Overall Risk	Medium
Probability	Low	Advised Action	To Plan
Severity	Medium		

Description

This report identifies hosts that have the DB2 Discovery Service running and accessible on the Internet.

This service has the potential to expose information about a client’s network on which this service is accessible, and the service itself can be used in UDP amplification attacks.

Assessment

The entries in this report are hosts that have the DB2 discovery service open towards the internet. DB2 is a family of related data management products by IBM. The Discovery Service is one service which is used for finding products of that family on the network. An attacker can abuse this service for DoS amplification and data leakage.

The likelihood is low.

The impact is set to medium as exploiting this service can result in data exfiltration. Additionally, the service can be used for DoS amplification attacks.

The overall risk is set to medium.

Recommendations

- Restrict access to internal networks.

References

- Shadow Server – Open DB2 Discovery Service Report https://www.shadowserver.org/what-we-do/network-reporting/open-db2-discovery-service-report/

Legend

Risk formula description by **ISACA:**
https://www.isaca.org/Journal/archives/2014/Volume-4/Pages/JOnline-An-Enhanced-Risk-Formula-for-Software-Security-Vulnerabilities.aspx?utm_referrer=
➔Risk = Likelihood * Impact

Enhanced risk formula:
RISK = CRITICALITY (Likelihood * Vulnerability Scores [CVSS]) * IMPACT

Overall category definition and explanation;

Overall Risk (likelihood * impact)
=> **Low**, **Medium**, **High**

Criticality (probability * severity)
=> **Low**, **Medium**, **High**

Severity (vulnerability CVSS grading - presents the **impact & capability of a threat**)
=> (Very Low), **Low**, **Medium**, **High**, (Very High)

Probability (statistical way of measuring **LIKELIHOOD)**

Impact (loss connected to the event occurrence)