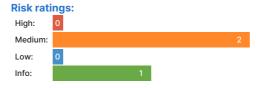


# **DNS Server Scanner Report**

### zonetransfer.me

### **Summary**





#### Scan information:

Start time: Mar 15, 2024 / 09:22:33 Finish time: Mar 15, 2024 / 09:22:35

Scan duration: 2 sec Tests performed: 3/3

Scan status: Finished

### **Findings**



# **DNS Server Zone Transfer Information Disclosure (AXFR)**

port 53/udp

We managed to extract the zone file from the nsztm2.digi.ninja. name server.

Below are the first 5 lines of the zone file:

zonetransfer.me. 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600

zonetransfer.me. 300 IN HINFO "Casio fx-700G" "Windows XP"

zonetransfer.me. 301 IN TXT "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VIMewxA"

zonetransfer.me. 7200 IN MX 0 ASPMX.L.GOOGLE.COM. zonetransfer.me. 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.

You can also see the entire zone file here.

### ✓ Details

### Vulnerability description:

The remote name server permits the execution of DNS zone transfers, a process that enables a malicious attacker to rapidly compile a list of potential targets. Furthermore, organizations frequently employ naming conventions that may inadvertently reveal a server's primary purpose, such as dev.example.com, staging.example.com, prod.example.com, and so forth.

### Risk description:

This data can be used by an attacker to gain insights about the network's structure and to find new potential targets.

### **Recommendation:**

Reconfigure the DNS server to only allow zone transfers from trusted IP addresses.



# **DNS Server Zone Transfer Information Disclosure (AXFR)**

port 53/udp

We managed to extract the zone file from the nsztm1.digi.ninja. name server.

Below are the first 5 lines of the zone file:

zonetransfer.me. 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600 3600

zonetransfer.me. 300 IN HINFO "Casio fx-700G" "Windows XP"

zonetransfer.me. 301 IN TXT "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VIMewxA"

zonetransfer.me. 7200 IN MX 0 ASPMX.L.GOOGLE.COM.

zonetransfer.me. 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.

You can also see the entire zone file here.

# Vulnerability description:

The remote name server permits the execution of DNS zone transfers, a process that enables a malicious attacker to rapidly compile a list of potential targets. Furthermore, organizations frequently employ naming conventions that may inadvertently reveal a server's primary purpose, such as dev.example.com, staging.example.com, prod.example.com, and so forth.

### Risk description:

This data can be used by an attacker to gain insights about the network's structure and to find new potential targets.

#### **Recommendation:**

Reconfigure the DNS server to only allow zone transfers from trusted IP addresses.

# Found 2 name servers for zonetransfer.me

Name Server	IP Address	Port
nsztm2.digi.ninja.	34.225.33.2	53
nsztm1.digi.ninja.	81.4.108.41	53

### ✓ Details

### Risk description:

No risk description to display.

#### **Recommendation:**

No recommendations to display.

# Scan coverage information

### List of tests performed (3/3)

- Searching for name servers of domain zonetransfer.me ...
- Attempting zone transfer against name server: nsztm2.digi.ninja....
- Attempting zone transfer against name server: nsztm1.digi.ninja....

# Scan parameters

Domain: zonetransfer.me