U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

J.D. Henry, M.B.A, CISSP, CISM, GCFA

Cyber Security Advisor

Cybersecurity Advisor Program

Cybersecurity and Infrastructure Security Agency

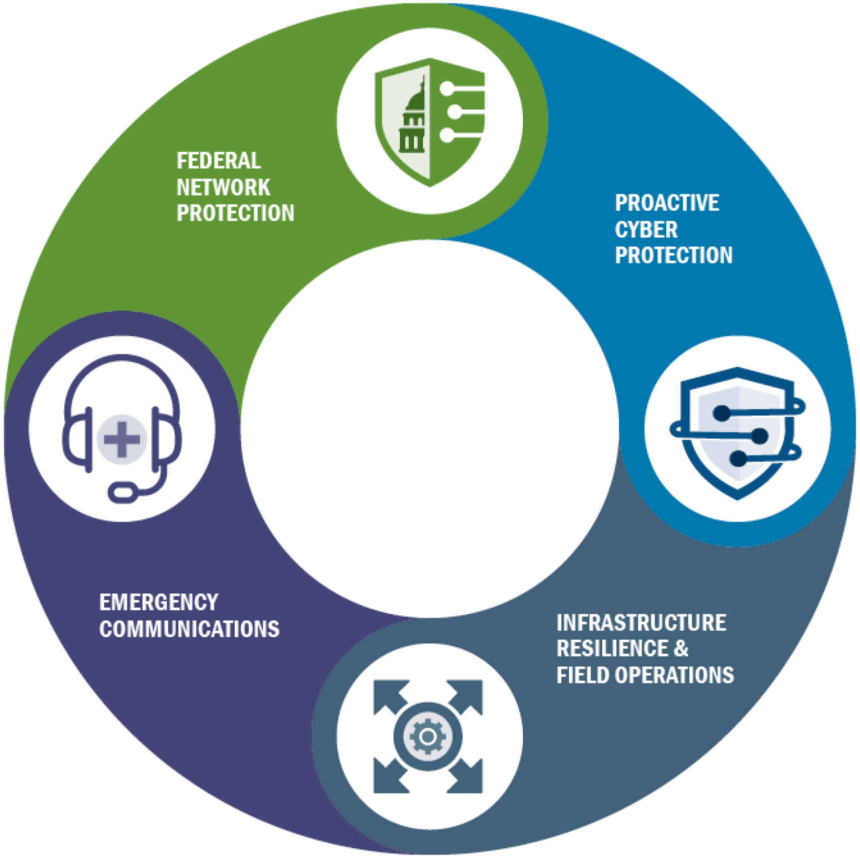
July 21, 2020

CISA

CYBER+INFRASTRUCTURE

The Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure


FEDERAL NETWORK PROTECTION
PROACTIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS

CISA
CYBER+INFRASTRUCTURE

CISA
Cybersecurity Advisor Program

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Advisor Program

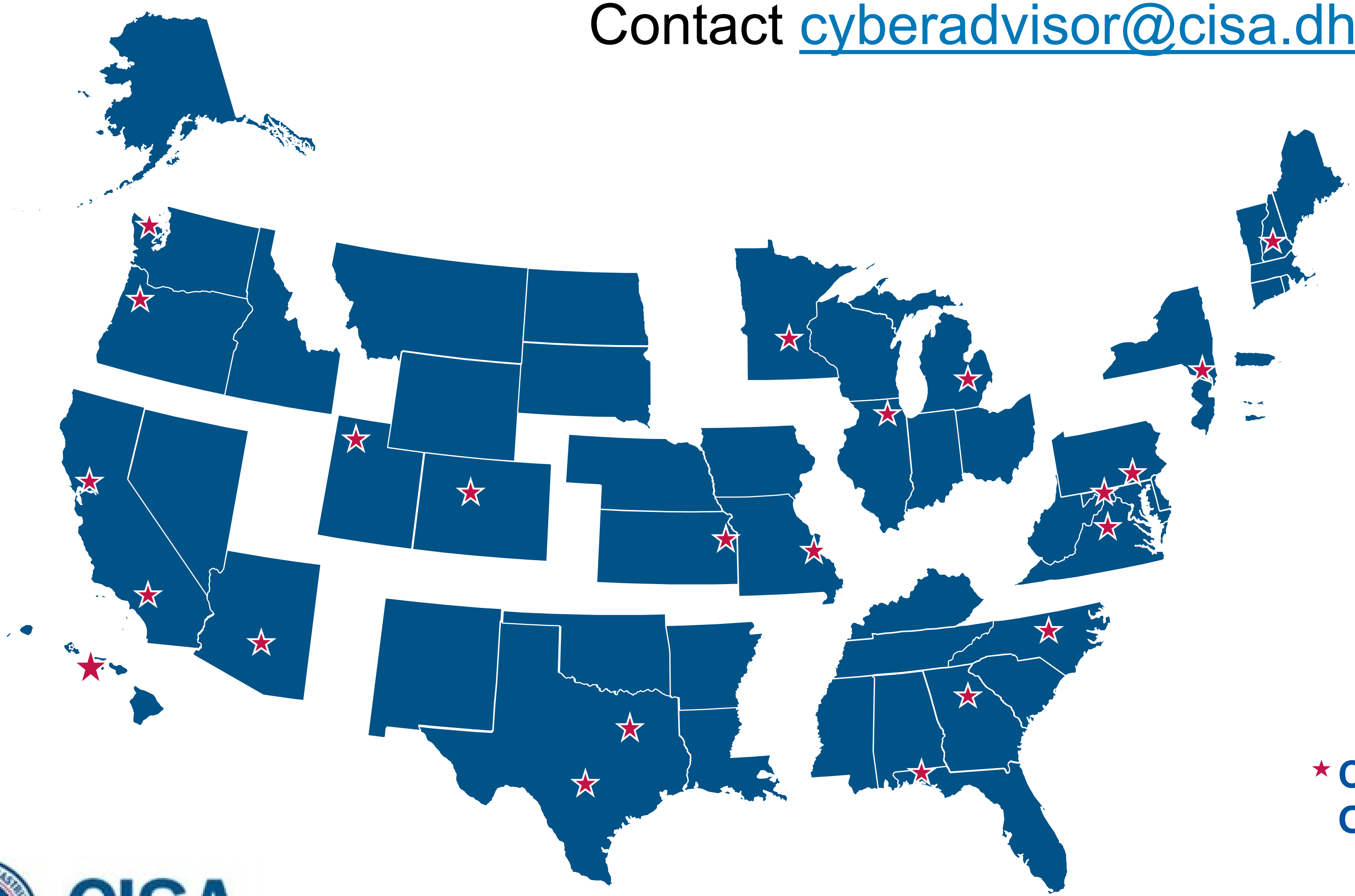
CISA mission: Lead the Nation's efforts to understand and manage risk to our critical infrastructure.

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

CSA Deployed Personnel

Contact cyberadvisor@cisa.dhs.gov

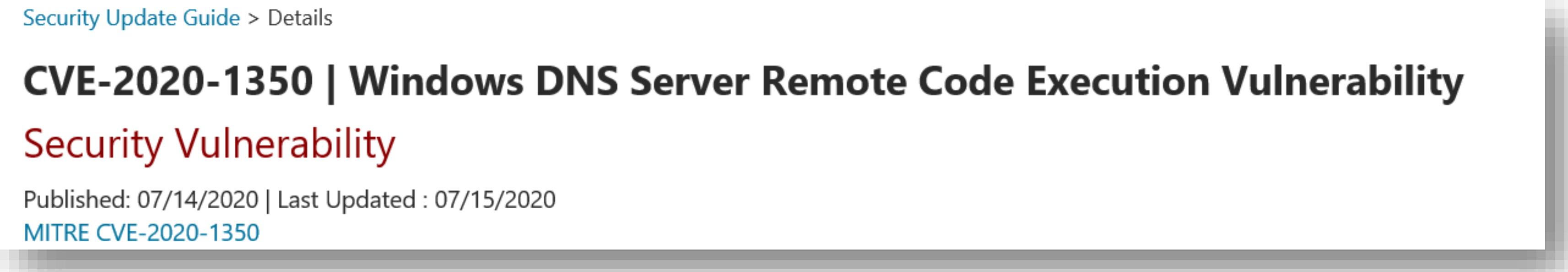


★ CSA Offices

CISA
CYBER+INFRASTRUCTURE

Who is targeting you?

CVE-2020-1350



Security Update Guide > Details

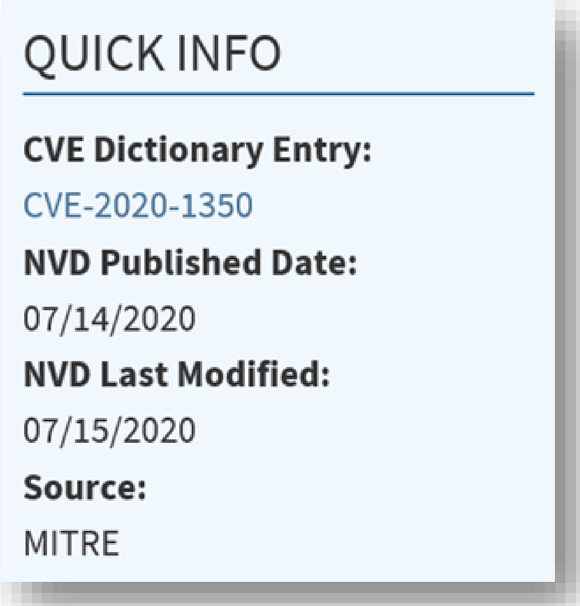
CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability

Security Vulnerability

Published: 07/14/2020 | Last Updated : 07/15/2020

MITRE CVE-2020-1350

Tuesday, July 14th, Microsoft released a security update to address a remote code execution vulnerability—CVE-2020-1350—in Windows Servers running the Domain Name System (DNS) role.



QUICK INFO

CVE Dictionary Entry:
CVE-2020-1350

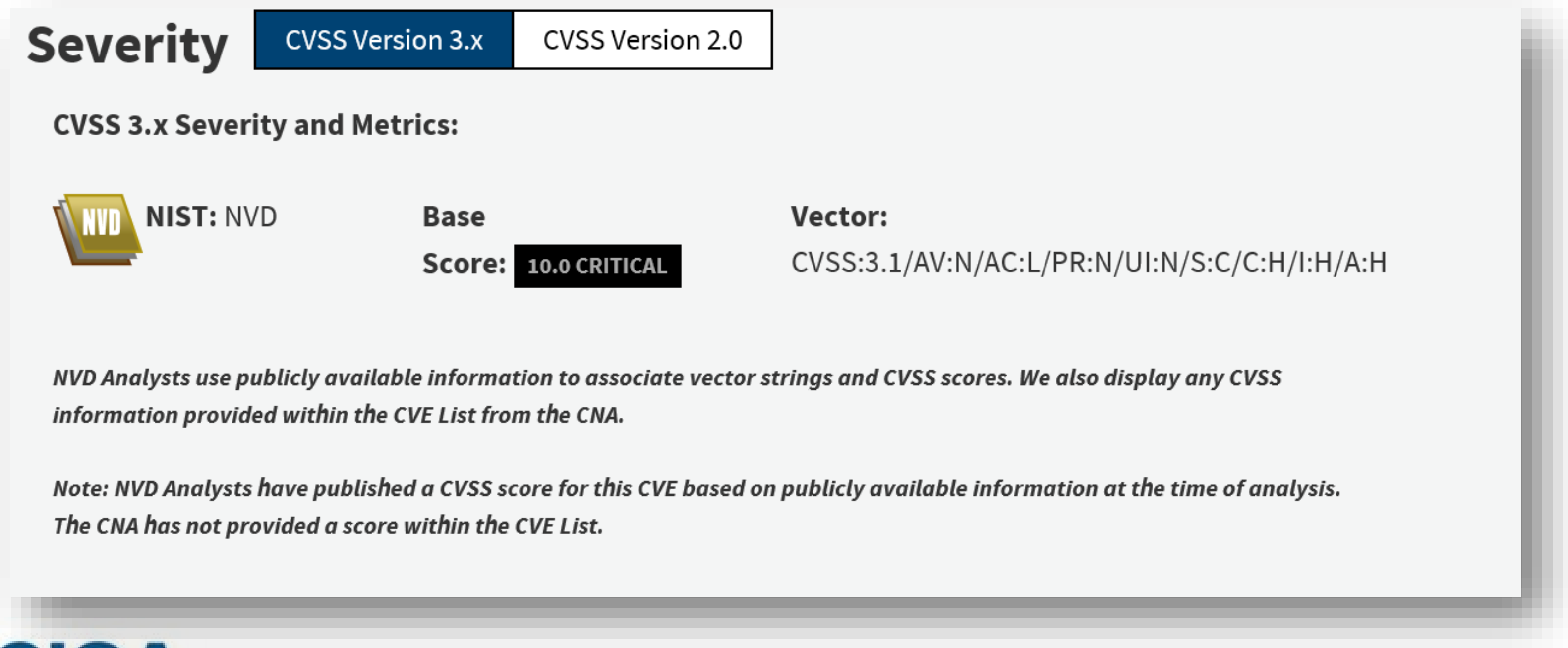
NVD Published Date:
07/14/2020

NVD Last Modified:
07/15/2020

Source:
MITRE

CVE-2020-1350

A remote attacker could exploit this vulnerability to take control of an affected system. This is considered a "*wormable*" vulnerability that affects all Windows Server versions.



CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 10.0 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

CVE-2020-1350

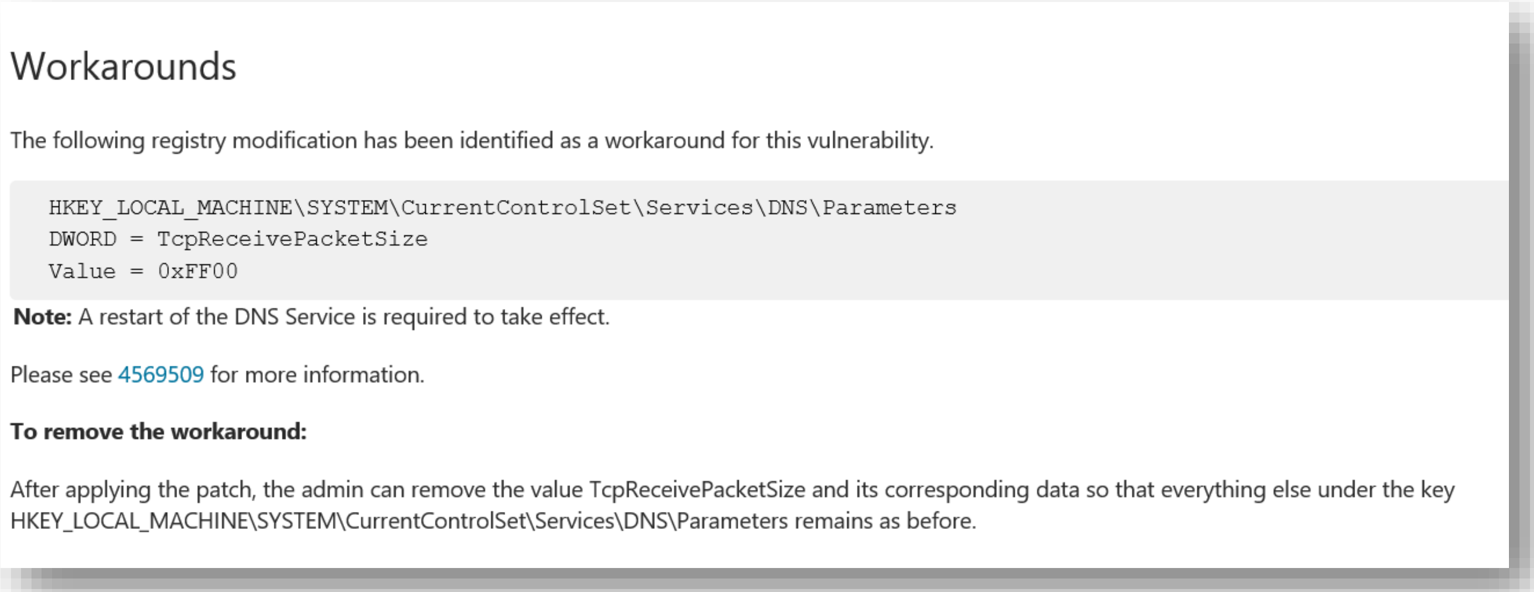
- The vulnerability effects all versions of Windows Server (2003, 2008, 2012, 2016, 2019, and Windows Server version 1903, 1909, and 2004).

- An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the local system account.

- When a Domain Controller running DNS is exploited, all Active Directory accounts would be quickly compromised.

CVE-2020-1350

The software patch addresses the critical vulnerability in Windows Server operating systems running DNS so prioritize updating those systems first. CISA also strongly urges that everyone apply this security update patch to all end points running Microsoft Windows Server operating systems.



Workarounds

The following registry modification has been identified as a workaround for this vulnerability.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
DWORD = TcpReceivePacketSize
Value = 0xFF00
```

Note: A restart of the DNS Service is required to take effect.

Please see 4569509 for more information.

To remove the workaround:

After applying the patch, the admin can remove the value TcpReceivePacketSize and its corresponding data so that everything else under the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters remains as before.

CISA
CYBER+INFRASTRUCTURE

CISA Service Offerings

If you are not a Cyber Hygiene (CyHy) customer, we encourage you to sign up for our network vulnerability scanning service at cisa.gov/cyber-resource-hub.

For this risk, our CyHy customers were scanned for this vulnerability and notified if they were at risk.

In some cases, we can notify CyHy customers before a vulnerability is public.

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic) ---------------------------
- External Dependencies Management (Strategic)-----------
- Cyber Infrastructure Survey (Strategic)------------------------
- Cybersecurity Evaluations Tool (Strategic/Technical)-----
- Phishing Campaign Assessment (Technical)----------------
- Vulnerability Scanning / Hygiene (Technical)----------------
- Validated Architecture Design Review (Technical)---------
- Risk and Vulnerability Assessment (Technical)-------------

TECHNICAL
(Network-Administrator Level)

Additional Documentation/Resources

https://nvd.nist.gov/vuln/detail/CVE-2020-1350

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350

https://cyber.dhs.gov/ed/20-03/

CISA
CYBER+INFRASTRUCTURE

Incident Reporting

CISA provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
  - cisaservicedesk@cisa.dhs.gov
  - WWW.CISA.GOV

Report Cyber Issue

When to Report:

If there is a suspected or confirmed cyber attack or incident that:

❖ Affects core government or critical infrastructure functions;

❖ Results in the loss of data, system availability; or control of systems;

❖ Indicates malicious software is present on critical systems

Malware Submission Process:

- Please send all submissions to the Advance Malware Analysis Center (AMAC) at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov

CISA
CYBER+INFRASTRUCTURE

Contacts and Questions?

Joseph “JD” Henry

Region VII Cybersecurity Advisor

(202) 860-7546

Joseph.Henry@cisa.dhs.gov

For inquiries or further information, contact cyberadvisor@cisa.dhs.gov

CISA
CYBER+INFRASTRUCTURE