

# Collaboration between JPRS and national CERT

24 May 2022

Pre-ICANN74 ccTLD News Session - Cybersecurity

Yasuhiro Orange Morishita

Japan Registry Services Co., Ltd. (JPRS)

# Who am I?

- Yasuhiro Orange Morishita

- Technical public relations

- Providing information and capacity building on DNS and domain name related technologies
- Cooperation with related organizations when security incident occurs

- (Formerly) system/network engineer and DNS researcher

- Co-author of RFC 4074 (in 2005)

- “Common Misbehavior Against DNS Queries for IPv6 Addresses”

- » Such behavior can block IPv4 communication that should actually be available, cause a significant delay in name resolution, or even make a denial of service attack

- WIDE Project member since 1990 (and present)



# Situations in Japan (1/2)

- National CERT of Japan: JPCERT/CC and NISC
  - Work together as a national CERT since 2015
- JPCERT/CC: a “CSIRT of CSIRTs” in the Japanese community
  - Established in 1996 as “JaPan  
Computer Emergency Response  
Team Coordination Center”
    - The first CSIRT established in Japan
  - Not a government agency
- NISC: a governmental CERT in Japan
  - Established in 2005 as “National  
Information Security Center”
  - Re-organized in 2015 as “National  
center of Incident readiness and  
Strategy for Cybersecurity”,  
under the Japanese Cabinet

# Situations in Japan (2/2)

- Government has regulated name server function of .jp as a “specified domain name telecommunications service”
  - By revision of Telecommunications Business Law since 2015
  - It defines service outage of JP DNS
- Government does not regulate data entry function of .jp

# Collaboration between JPRS and JPCERT/CC

- Special collaboration team is formed by three JP\* parties in sharing security information
  - Triggered by the Kaminsky-style attacks security incident in 2008
  - Collaborative works for responding DNS-related security incidents
  - Information exchange by mailing list / face-to-face meetings
    - Both in normal times and in the event of security incidents
- Team members
  - JPRS (as domain name registry)
  - JPNIC (as network information center)
  - JPCERT/CC (as national CERT)

# Collaboration between JPRS and NISC

- NISC publishes “Critical Infrastructure Newsletter” periodically
  - NISC defines 14 “Critical Infrastructures”
    - Information & communication, Finance, Aviation, Airport, Railway, Electric power supply, Gas supply, Government & administration, Medical, Water, Logistics, Chemical industries, Credit card, Petroleum industries
  - Sharing security information related to critical infrastructures
- JPRS shares its security related advices to NISC for adding the link to its newsletter

# JPRS's Motivation for the collaboration

- Can deliver security information to related parties
  - Widely
    - JPRS can deliver security information to .JP registrars (about 600 entities)
      - Many of the registrars also provide DNS services
    - JPNIC can deliver security information to their members as a network information center
    - JPCERT/CC and NISC can deliver security information to community-wide
  - Easy to understand
    - JPRS performs technical verification of security information as a DNS operator, and advises to the community in Japanese (our local language!)

# Examples of collaborative work

- Jointly advise to the Japanese Internet community
  - **DNS software vulnerabilities**
    - Target: BIND and some major DNS software
    - Coordination for mutual links for each document
    - Share and technical review of each document
  - **Critical security incidents**
    - The Kaminsky-style attacks (2008)
    - Domain name hijacking (2014)
      - By unauthorized rewriting of registration information
      - nikkei.com (famous business newspaper's company), and well-known gTLD domains
    - Zone data breach from authoritative servers (2016)
      - By zone transfer requests to authoritative servers with improper settings



# Examples of collaborative work (CVE-2021-25219: BIND vulnerability)

## • Advice of JPCERT/CC

**概要**

ISC BIND 9には、lame cacheの設計の問題による、サービス運用妨害 (DoS) の脆弱性があります。結果として、遠隔の第三者によって送信された細工されたクエリを処理することで、クライアントでの処理が遅延し、タイムアウトが発生する可能性があります。

対象となるバージョンは次のとおりです。

- BIND Supported Preview Edition 9.16.8-S1から9.16.21-S1までのバージョン
- BIND Supported Preview Edition 9.9.3-S1から9.11.35-S1までのバージョン
- BIND 9.12.0から9.16.21までのバージョン
- BIND 9.3.0から9.11.35までのバージョン
- BIND development branch 9.17.0から9.17.18までのバージョン

この脆弱性を解決するためには、ISCが提供する情報を参照してください。

関連文書 (日本語)

株式会社日本レジストリサービス (JPRS)  
BIND 9.xの脆弱性 (パフォーマンスの低下) について (CVE-2021-25219) - バージョンアップを推奨 -  
<https://jprs.jp/tech/security/2021-10-28-bind9-vuln-lamecache.html>

## • Advice of NISC

◆◆ NISC重要インフラニュースレター ◆◆  
(2021年11月9日発行 第297号)  
発行：NISC重要インフラグループ

1. チェックが必要な情報

(3) その他

CLUSTERPRO X および EXPRESSCLUSTER X における複数の脆弱性(JVN)(10/29)  
<https://jvn.jp/jp/JVN69304877/>  
※CVSSv3では基本値「10.0」となっています。

Android アプリ「メルカリ(メルペイ)-フリマアプリ&スマホ決済」における Intent の取り扱い不備に関する脆弱性(JVN)(10/29)  
<https://jvn.jp/jp/JVN49465877/>  
※CVSSv3では基本値「7.4」となっています。

ESET Cyber Security および ESET Endpoint シリーズにおけるサービス運用妨害 (DoS) の脆弱性(JVN)(10/29)  
<https://jvn.jp/jp/JVN60553023/>

ISC BINDにサービス運用妨害 (DoS) の脆弱性(JVN)(10/28)  
<https://jvn.jp/vu/JVNVU01101819/>

BIND 9.xの脆弱性 (パフォーマンスの低下) について (CVE-2021-25219) (JPRS) (10/28)  
<https://jprs.jp/tech/security/2021-10-28-bind9-vuln-lamecache.html>

Information that needs to be checked

Link to JPRS advice

# Thank you!

Yasuhiro Orange Morishita  
<yasuhiro@jprs.co.jp>