

# GLUON UPDATE! 2022

WHAT'S NEW SINCE WBMV10

LINUS LÜSSING (T\_X)

WIRELESS BATTLEMESH V14, ROME

SEPTEMBER 20, 2022

1 What is Gluon

2 What's new since WBMv10

3 CVE-2022-24884

# WHAT IS GLUON

# What is Gluon

# What is Gluon

- A modular firmware framework for mesh networks

# What is Gluon

- A modular firmware framework for mesh networks
- Based on OpenWrt

# What is Gluon

- A modular firmware framework for mesh networks
- Based on OpenWrt
- First release: v2014.1 in March 2014

# What is Gluon

- A modular firmware framework for mesh networks
- Based on OpenWrt
- First release: v2014.1 in March 2014
- Popular in Freifunk communities



# Main Features

# Main Features

- Integrates mesh routing protocols:
  - ▶ batman-adv
  - ▶ Babel + l3roamd (IPv6 only)

# Main Features

- Integrates mesh routing protocols:
  - ▶ batman-adv
  - ▶ Babel + l3roamd (IPv6 only)
- Integrates VPN protocols:
  - ▶ **fastd**
  - ▶ tunneldigger L2TP
  - ▶ Wireguard

# Main Features

- Integrates mesh routing protocols:
  - ▶ batman-adv
  - ▶ Babel + I3roamd (IPv6 only)
- Integrates VPN protocols:
  - ▶ **fastd**
  - ▶ tunneldigger L2TP
  - ▶ Wireguard
- respondd for statistics
  - ▶ lightweight, JSON in UDP

# Main Features

- Integrates mesh routing protocols:
  - ▶ batman-adv
  - ▶ Babel + I3roamd (IPv6 only)
- Integrates VPN protocols:
  - ▶ **fastd**
  - ▶ tunneldigger L2TP
  - ▶ Wireguard
- respondd for statistics
  - ▶ lightweight, JSON in UDP
- Autoupdater

# Main Features

- Integrates mesh routing protocols:
  - ▶ batman-adv
  - ▶ Babel + I3roamd (IPv6 only)
- Integrates VPN protocols:
  - ▶ **fastd**
  - ▶ tunneldigger L2TP
  - ▶ Wireguard
- respondd for statistics
  - ▶ lightweight, JSON in UDP
- Autoupdater
- More details: See our previous presentation at WBMv10

# WHAT'S NEW SINCE WBMV10





- #Nodes At Freifunk: 44k (2017: 35k)

- #Nodes At Freifunk: 44k (2017: 35k)
- Releases since 2017 (since 2014/total): 36 (59)

- #Nodes At Freifunk: 44k (2017: 35k)
- Releases since 2017 (since 2014/total): 36 (59)
- Git commits v2017.1..v2022.1 (since 2014/total): 2214 (5211)

- #Nodes At Freifunk: 44k (2017: 35k)
- Releases since 2017 (since 2014/total): 36 (59)
- Git commits v2017.1..v2022.1 (since 2014/total): 2214 (5211)
- #Supported devices in v2022.1: 174 (v2017.1: 100, v2021.1: 189)

# OpenWrt Base Updates

# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01

# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01
- Gluon v2020.1 → OpenWrt 19.07

# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01
- Gluon v2020.1 → OpenWrt 19.07
- Gluon v2022.1 → OpenWrt 22.03



# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01
- Gluon v2020.1 → OpenWrt 19.07
- Gluon v2022.1 → OpenWrt 22.03
  - ▶ swconfig → DSA

# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01
- Gluon v2020.1 → OpenWrt 19.07
- Gluon v2022.1 → OpenWrt 22.03
  - ▶ swconfig → DSA
  - ▶ ar71xx → ath79
    - ⇒ retesting all devices

# OpenWrt Base Updates

- Gluon v2017.1 → LEDE 17.01
- Gluon v2020.1 → OpenWrt 19.07
- Gluon v2022.1 → OpenWrt 22.03
  - ▶ swconfig → DSA
  - ▶ ar71xx → ath79
    - ⇒ retesting all devices
  - ▶ 4MB flash or 32MB RAM devices removed

# New VPN Protocol Support

# New VPN Protocol Support

- tunneldigger L2TP (v2017.1)
  - ▶ kernelspace, unencrypted, unauthenticated
  - ▶ over IPv4 only

# New VPN Protocol Support

- tunneldigger L2TP (v2017.1)
  - ▶ kernelspace, unencrypted, unauthenticated
  - ▶ over IPv4 only
- fastd L2TP (v2022.1)
  - ▶ kernelspace, unencrypted
  - ▶ setup authenticated by fastd, reuses existing key infrastructure

# New VPN Protocol Support

- tunneldigger L2TP (v2017.1)
  - ▶ kernelspace, unencrypted, unauthenticated
  - ▶ over IPv4 only
- fastd L2TP (v2022.1)
  - ▶ kernelspace, unencrypted
  - ▶ setup authenticated by fastd, reuses existing key infrastructure
- Wireguard (v2022.1)
  - ▶ kernelspace, encrypted, authenticated
  - ▶ more header overhead (VXLAN)

# New Mesh Protocols



- Babel + l3roamd – experimental, IPv6 only (v2018.2)

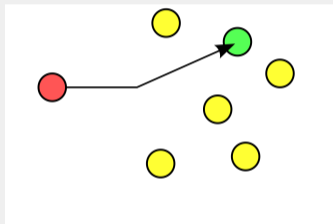
- Babel + l3roamd – experimental, IPv6 only (v2018.2)
  - ▶ more testers welcome

- Babel + l3roamd – experimental, IPv6 only (v2018.2)
  - ▶ more testers welcome
- BATMAN V – experimental/partial (2017.1.2)

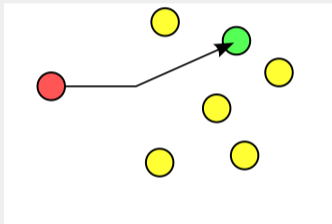
- Babel + l3roamd – experimental, IPv6 only (v2018.2)
  - ▶ more testers welcome
- BATMAN V – experimental/partial (2017.1.2)
- (upcoming: OLSRv2 - first PR thanks to FunkFeuer Graz)

# Directed Multicast (v2021.1)

# Directed Multicast (v2021.1)

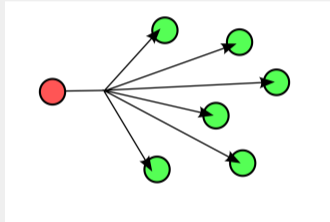
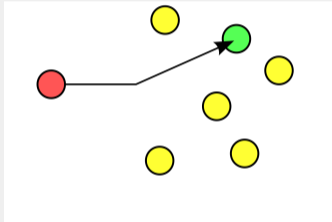


# Directed Multicast (v2021.1)



■ Unicast

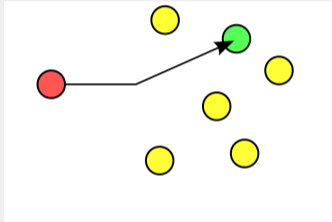
# Directed Multicast (v2021.1)



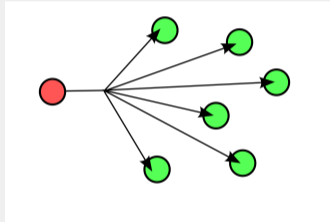
■ Unicast



# Directed Multicast (v2021.1)

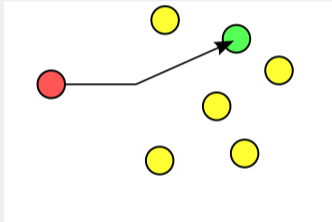


■ Unicast

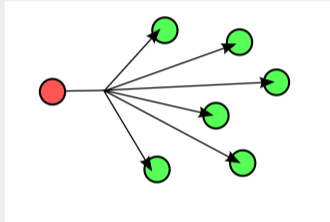


■ Broadcast

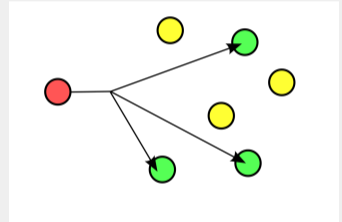
# Directed Multicast (v2021.1)



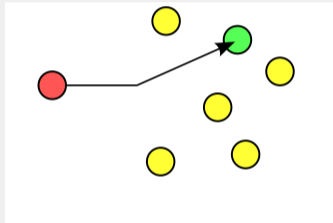
■ Unicast



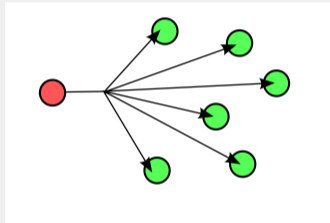
■ Broadcast



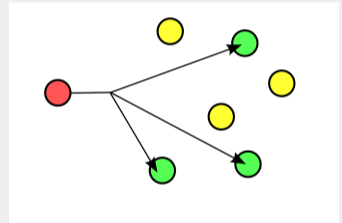
# Directed Multicast (v2021.1)



■ Unicast

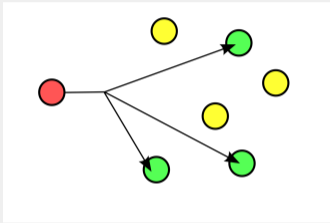


■ Broadcast

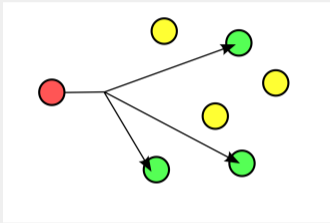


■ Multicast

# Directed Multicast (v2021.1)

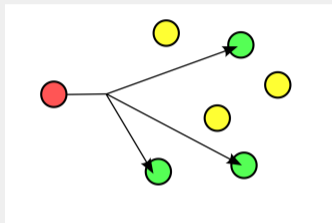


# Directed Multicast (v2021.1)



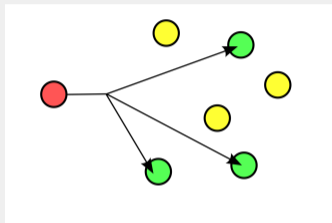
- batman-adv learns multicast listeners

# Directed Multicast (v2021.1)



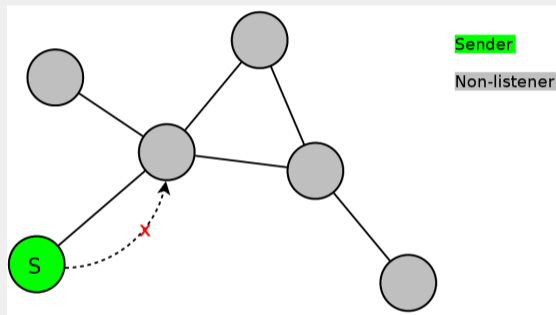
- batman-adv learns multicast listeners
- via IGMP/MLD snooping (through the Linux bridge)

# Directed Multicast (v2021.1)



- batman-adv learns multicast listeners
- via IGMP/MLD snooping (through the Linux bridge)
- applied to IPv6 link-local multicast in Gluon  
(routeable multicast: PR available, excluding multicast router support)

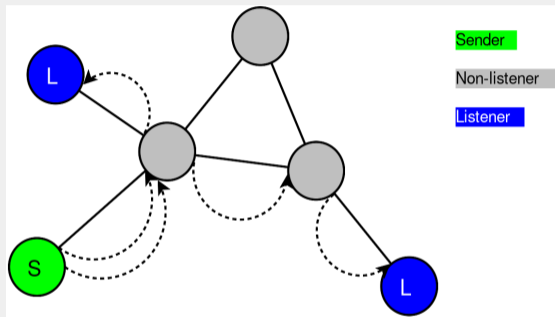
# Directed Multicast (v2021.1)



- If #listener-nodes = 0:
  - ▶ Drop

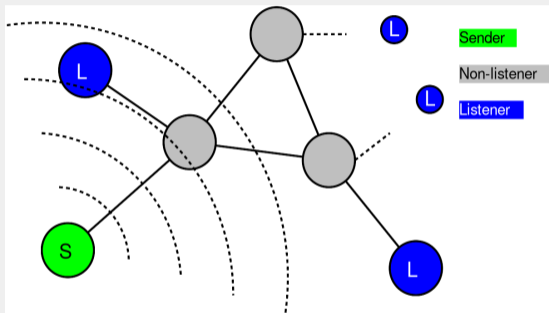


# Directed Multicast (v2021.1)



- Else if #listener-nodes  $\leq 16$ :
  - ▶ Unicast transmission(s)  
→ (typ.) higher datarate, ARQ (retries)

# Directed Multicast (v2021.1)



■ Else, #listener-nodes > 16:

- ▶ Broadcast fallback (ICMPv6) or filtered (by ebttables)

# Directed Multicast (v2021.1)

Advantages:

## Advantages:

- Less ICMPv6 Neighbor Discovery overhead:

## Advantages:

- Less ICMPv6 Neighbor Discovery overhead:
  - ▶ Duplicate Address Detection: typ. 0 listeners

## Advantages:

- Less ICMPv6 Neighbor Discovery overhead:
  - ▶ Duplicate Address Detection: typ. 0 listeners
  - ▶ Neighbor Solicitation: typ. 1 listener

## Advantages:

- Less ICMPv6 Neighbor Discovery overhead:
  - ▶ Duplicate Address Detection: typ. 0 listeners
  - ▶ Neighbor Solicitation: typ. 1 listener
- relaxed firewall rules for IPv6 link-local multicast

## ■ Example application: **Syncthing**

The screenshot displays the Syncthing web interface for 'This computer'. The interface is divided into several sections:

- Top Bar:** Shows the Syncthing logo, the current device name 'This computer', and navigation options for 'English', 'Help', and 'Actions'.
- Folders:** A section titled 'Folders' containing a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder list are three buttons: 'Pause All', 'Rescan All', and 'Add Folder'.
- This Device:** A section titled 'This Device' showing system statistics for 'This computer':
  - Download Rate: 0 B/s (0 B)
  - Upload Rate: 0 B/s (0 B)
  - Local State (Total): 0 B, 0 B, -0 B
  - Listeners: 2/3
  - Discovery: 3/5
  - Uptime: 38m
  - Version: v1.7.1, Windows (32 bit)
- Remote Devices:** A section titled 'Remote Devices' with three buttons: 'Pause All', 'Recent Changes', and 'Add Remote Device'.
- Footer:** A navigation bar with links for 'Home page', 'Documentation', 'Support', 'Statistics', 'Changelog', 'Bugs', and 'Source Code', along with a 'Twitter' link.




# Directed Multicast (v2021.1)

- Example application: **Syncthing**
- Synchronizes folders

The screenshot displays the Syncthing web interface for 'This computer'. The interface is divided into several sections:

- Folders:** Shows a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder list are three buttons: 'Pause All', 'Rescan All', and 'Add Folder'.
- This Device:** A summary panel for 'This computer' with the following statistics:
  - Download Rate: 0 B/s (0 B)
  - Upload Rate: 0 B/s (0 B)
  - Local State (Total): 0 files, 0 folders, -0 B
  - Listeners: 2/3
  - Discovery: 3/5
  - Uptime: 38m
  - Version: v1.7.1, Windows (32 bit)
- Remote Devices:** A section with three buttons: 'Pause All', 'Recent Changes', and 'Add Remote Device'.

At the bottom of the interface, there is a navigation bar with links for Home page, Documentation, Support, Statistics, Changelog, Bugs, and Source Code, along with a Twitter icon.

 CC BY 4.0, Wikipedia

# Directed Multicast (v2021.1)

- Example application: **Syncthing**
- Synchronizes folders
- Uses Bittorrent protocol for syncing

The screenshot displays the Syncthing web interface for 'This computer'. The top navigation bar includes the Syncthing logo, the current device name, and options for language (English), help, and actions. The main content area is divided into three sections:

- Folders:** Shows a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder name are three buttons: 'Pause All', 'Rescan All', and 'Add Folder'.
- This Device:** A summary panel for 'This computer' displaying various statistics:

Download Rate	0 B/s (0 B)
Upload Rate	0 B/s (0 B)
Local State (Total)	0 0 0 -0 B
Listeners	2/3
Discovery	3/5
Uptime	38m
Version	v1.7.1, Windows (32 bit)
- Remote Devices:** A section with three buttons: 'Pause All', 'Recent Changes', and 'Add Remote Device'.

The footer contains navigation links for Home page, Documentation, Support, Statistics, Changelog, Bugs, and Source Code, along with a Twitter icon.

 CC BY 4.0, Wikipedia

# Directed Multicast (v2021.1)

- Example application: **Syncthing**
- Synchronizes folders
- Uses Bittorrent protocol for syncing
- Available on: Mac OS X, Windows, Linux, FreeBSD, Solaris, OpenBSD, Android

The screenshot displays the Syncthing web interface for 'This computer'. At the top, there is a navigation bar with the Syncthing logo, the text 'This computer', and menu items for 'English', 'Help', and 'Actions'. The main content area is divided into three sections:

- Folders:** Shows a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder name are three buttons: 'Pause All', 'Rescan All', and 'Add Folder'.
- This Device:** A summary panel for 'This computer' displaying various system metrics:

Download Rate	0 B/s (0 B)
Upload Rate	0 B/s (0 B)
Local State (Total)	0 0 0 -0 B
Listeners	2/3
Discovery	3/5
Uptime	38m
Version	v1.7.1, Windows (32 bit)
- Remote Devices:** A section for managing other devices, featuring buttons for 'Pause All', 'Recent Changes', and 'Add Remote Device'.

At the bottom of the interface, there is a footer with links for 'Home page', 'Documentation', 'Support', 'Statistics', 'Changelog', 'Bugs', and 'Source Code', along with a 'Twitter' icon.

# Directed Multicast (v2021.1)

- Example application: **Syncthing**
- Synchronizes folders
- Uses Bittorrent protocol for syncing
- Available on: Mac OS X, Windows, Linux, FreeBSD, Solaris, OpenBSD, Android
- Has local peer discovery feature

The screenshot displays the Syncthing web interface for 'This computer'. At the top, there is a navigation bar with the Syncthing logo, the text 'This computer', and menu items for 'English', 'Help', and 'Actions'. The main content area is divided into three sections:

- Folders:** Shows a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder name are three buttons: 'Pause All', 'Rescan All', and '+ Add Folder'.
- This Device:** A summary panel for the local device. It lists several metrics:
  - Download Rate: 0 B/s (0 B)
  - Upload Rate: 0 B/s (0 B)
  - Local State (Total): 0 files, 0 folders, -0 B
  - Listeners: 2/3
  - Discovery: 3/5
  - Uptime: 38m
  - Version: v1.7.1, Windows (32 bit)
- Remote Devices:** A section for managing other devices, containing three buttons: 'Pause All', 'Recent Changes', and '+ Add Remote Device'.

At the bottom of the interface, there is a footer with links for 'Home page', 'Documentation', 'Support', 'Statistics', 'Changelog', 'Bugs', and 'Source Code', along with a 'Twitter' icon.

# Directed Multicast (v2021.1)

- Example application: **Syncthing**
- Synchronizes folders
- Uses Bittorrent protocol for syncing
- Available on: Mac OS X, Windows, Linux, FreeBSD, Solaris, OpenBSD, Android
- Has local peer discovery feature
  - ▶ Multicast address (default):  
ff12::8384

The screenshot displays the Syncthing web interface for 'This computer'. The top navigation bar includes the Syncthing logo, the current computer name, and options for language (English), help, and actions. The main content area is divided into two sections: 'Folders' and 'This Device'. The 'Folders' section shows a single folder named 'Default Folder' with a status of 'Unshared'. Below the folder name are three buttons: 'Pause All', 'Rescan All', and 'Add Folder'. The 'This Device' section provides a summary of system metrics: Download Rate (0 B/s), Upload Rate (0 B/s), Local State (Total) (0), Listeners (2/3), Discovery (3/5), Uptime (38m), and Version (v1.7.1, Windows (32 bit)). Below this is a 'Remote Devices' section with buttons for 'Pause All', 'Recent Changes', and 'Add Remote Device'. The footer contains links for Home page, Documentation, Support, Statistics, Changelog, Bugs, and Source Code, along with a Twitter icon.

# Further Filtering & Separations

- gluon-ebtables-limit-arp (v2018.1)

## Further Filtering & Separations

- `gluon-ebtables-limit-arp` (v2018.1)
- `gluon-ebtables-source-filter` (v2017.1)



## Further Filtering & Separations

- `gluon-ebtables-limit-arp` (v2018.1)
- `gluon-ebtables-source-filter` (v2017.1)
- `VXLAN on wired-mesh` (v2018.1)

# Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting

## Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting
- Typical per domain settings:

# Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting
- Typical per domain settings:
  - ▶ mesh-id

# Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting
- Typical per domain settings:
  - ▶ mesh-id
  - ▶ domain\_seed → used for vxlan-id

# Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting
- Typical per domain settings:
  - ▶ mesh-id
  - ▶ domain\_seed → used for vxlan-id
  - ▶ prefix4/prefix6

# Multi-Domain support (v2018.1)

- Eased community (broadcast domain) splitting
- Typical per domain settings:
  - ▶ mesh-id
  - ▶ domain\_seed → used for vxlan-id
  - ▶ prefix4/prefix6
  - ▶ mesh-vpn gateways





- Allows switching domain at specific time

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:
  - ▶ IBSS  $\Rightarrow$  11s (w/o forwarding)

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:
  - ▶ IBSS  $\Rightarrow$  11s (w/o forwarding)
  - ▶ batman-adv compat14 (batman-adv  $\leq$  v2013.4)  $\Rightarrow$  compat15 ( $\geq$  2014.1)

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:
  - ▶ IBSS  $\Rightarrow$  11s (w/o forwarding)
  - ▶ batman-adv compat14 (batman-adv  $\leq$  v2013.4)  $\Rightarrow$  compat15 ( $\geq$  2014.1)
    - both IBSS and compat14 removed in Gluon v2020.1

- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:
  - ▶ IBSS  $\Rightarrow$  11s (w/o forwarding)
  - ▶ batman-adv compat14 (batman-adv  $\leq$  v2013.4)  $\Rightarrow$  compat15 ( $\geq$  2014.1)
    - both IBSS and compat14 removed in Gluon v2020.1
  - ▶ BATMAN IV  $\Leftrightarrow$  BATMAN V



- Allows switching domain at specific time
- Useful for otherwise incompatible migrations
- Examples:
  - ▶ IBSS  $\Rightarrow$  11s (w/o forwarding)
  - ▶ batman-adv compat14 (batman-adv  $\leq$  v2013.4)  $\Rightarrow$  compat15 ( $\geq$  2014.1)
    - both IBSS and compat14 removed in Gluon v2020.1
  - ▶ BATMAN IV  $\Leftrightarrow$  BATMAN V
  - ▶ WLAN channel

# WLAN encryption (v2020.2)

- WPA3

- WPA3
  - ▶ SAE (Simultaneous Authentication of Equals) on private-wifi

- WPA3

- ▶ SAE (Simultaneous Authentication of Equals) on private-wifi
- ▶ OWE (Opportunistic Wireless Encryption) on client-wifi

## ■ WPA3

- ▶ SAE (Simultaneous Authentication of Equals) on private-wifi
- ▶ OWE (Opportunistic Wireless Encryption) on client-wifi
- ▶ Management Frame Protection

- WPA3
  - ▶ SAE (Simultaneous Authentication of Equals) on private-wifi
  - ▶ OWE (Opportunistic Wireless Encryption) on client-wifi
  - ▶ Management Frame Protection
- SAE on mesh

# WLAN encryption (v2020.2)

- WPA3
  - ▶ SAE (Simultaneous Authentication of Equals) on private-wifi
  - ▶ OWE (Opportunistic Wireless Encryption) on client-wifi
  - ▶ Management Frame Protection
- SAE on mesh
  - ▶ part of 802.11s standard



- WPA3
  - ▶ SAE (Simultaneous Authentication of Equals) on private-wifi
  - ▶ OWE (Opportunistic Wireless Encryption) on client-wifi
  - ▶ Management Frame Protection
- SAE on mesh
  - ▶ part of 802.11s standard
  - ▶ shared secret, unsuitable for public mesh networks

**CVE-2022-24884**



© neilmadden.blog

- Bug in ECDSA signature validation for autoupdater (ecdsautils)



© neilmadden.blog

# Psychic Paper

- Bug in ECDSA signature validation for autoupdater (ecdsautils)
- Very similar to Java's recent CVE-2022-21449, published: 19 April



© neilmadden.blog

# Psychic Paper

- Bug in ECDSA signature validation for autoupdater (ecdsautils)
- Very similar to Java's recent CVE-2022-21449, published: 19 April
- Accepts 000...0 as valid signature



© neilmadden.blog

- Bug in ECDSA signature validation for autoupdater (ecdsautils)
- Very similar to Java's recent CVE-2022-21449, published: 19 April
- Accepts 000...0 as valid signature
- Technical details:  
<https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/>



© neilmadden.blog

*Example:*

- <https://git.chaotikum.org/freifunk-luebeck/site-ffhl/-/blob/master/site.conf>
- <https://firmware.luebeck.freifunk.net/0.14.2/images/sysupgrade/>  
vs.:
- <https://firmware.luebeck.freifunk.net/0.15.2/images/sysupgrade/>



# Timeline

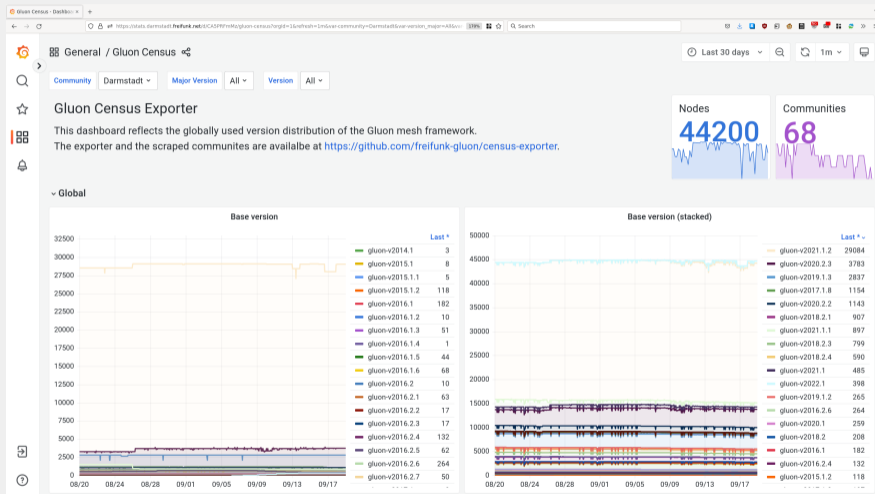
- Discovery: 20 April, by Matthias Schiffer (NeoRaider)

- Discovery: 20 April, by Matthias Schiffer (NeoRaider)
- Fix: 20 April, by NeoRaider

- Discovery: 20 April, by Matthias Schiffer (NeoRaider)
- Fix: 20 April, by NeoRaider
- Pre-announcement: 2 May

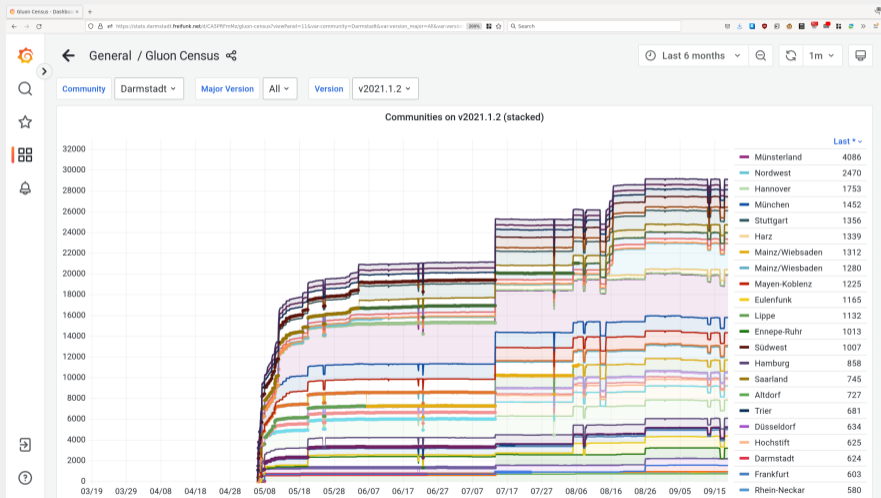
- Discovery: 20 April, by Matthias Schiffer (NeoRaider)
- Fix: 20 April, by NeoRaider
- Pre-announcement: 2 May
- Publication + Gluon release(s): 5 May

# Gluon Census

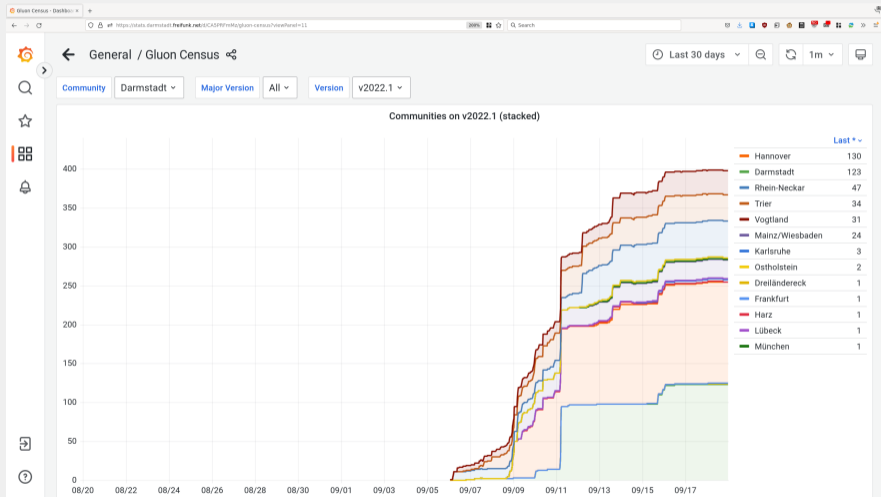


■ <https://github.com/freifunk-gluon/census-exporter>

# Gluon Census

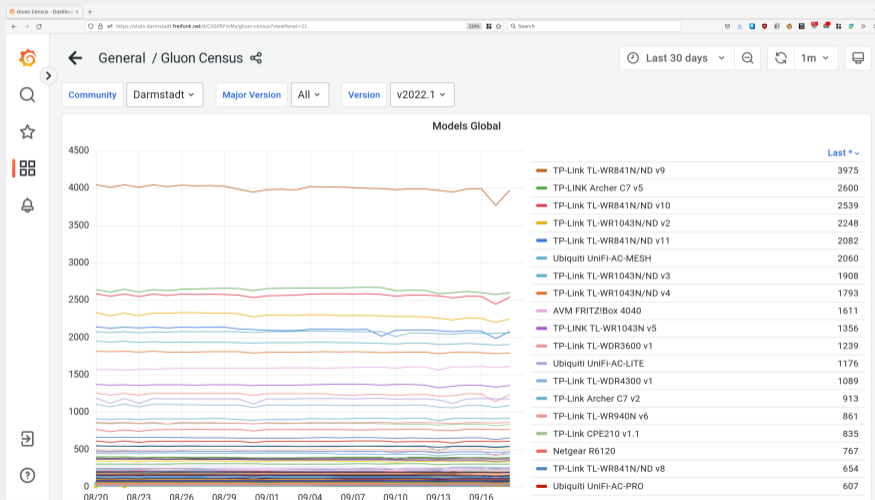


# Gluon Census





# Gluon Census



# Thx, Questions?

- <https://github.com/freifunk-gluon/gluon>
- Matrix: #gluon:hackint.org
- IRC: #gluon on hackint.org
- Mailinglist: gluon@luebeck.freifunk.net

License:  – CC-BY-SA-4.0, unless noted otherwise