# The Agricultural Data Arms Race:

## Exploiting a Tractor Load of Vulnerabilities In The Global Food Supply Chain.

(in good faith)

SICK.CODES

A man, “Using a hand tractor for cultivation. Falls City Farmsteads, Nebraska”

Rothstein, Arthur, 1915-1985, photographer (Public Domain)

# John Deere 7450 ProDrive Forage Harvester

# Disclaimer

- None of research was paid for
- All research was done in good faith
- Nothing today represents our employers, past employers, or future employers
- None of us are under gag orders*
- All content in the slides is CC0
- All trademarks, logos and brand names are the property of their respective owners.

# Who am I?

Sick Codes - good hackerman

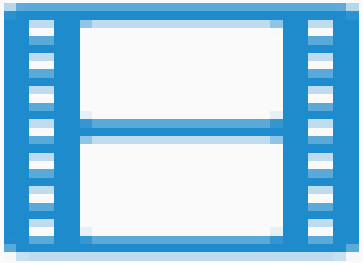
https://github.com/sickcodes

https://twitter.com/sickcodes

https://linkedin.com/in/sickcodes

https://sick.codes

# Why is this important?



# Scnenarios

- “The sprayers are programmed by the hacker to unevenly spray the chemicals on the crops, applying ten times the chemical on certain parts of the field, and a tenth the dose on other parts.”

# Skewed risks

- Denial of Service BIG impact

- “hacker uploads a firmware update that inserts an offset into the GPS locations used by the target.”

# Real threats

- “offset of (say) 100 yards North of where it should be. The target navigates itself onto a highway, into a river, through a fence, over a cliff, or whatever. Target is destroyed,”

Conor Cagney: https://sick.codes/leaky-john-deere-apis-serious-food-supply-chain-vulnerabilities-discovered-by-sick-codes-kevin-kenney-willie-cade/#comment-41658

# More Real threats

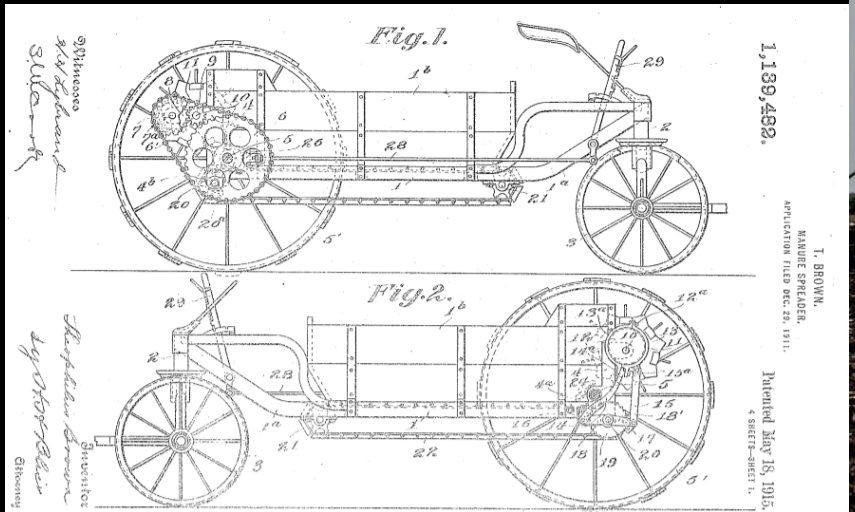
- “The sprayers are programmed by the hacker to unevenly spray the chemicals on the crops, applying ten times the chemical on certain parts of the field, and a tenth the dose on other parts.”

# Why did we even look at Ag?

Nobody else was.

# Willie Cade

Grandson of Theo Brown who was spent 30 years on John Deere Board.




# Kevin Kenney

- Nebraska
- Engineer
- Farmer
- Photographer: Walker Pickering for Bloomberg Businessweek

# The hackers

- Sick Codes https://twitter.com/sickcodes
- wabaf3t https://twitter.com/wabafet1
- D0rkerDevil https://twitter.com/D0rkerDevil
- johnjhacking https://twitter.com/johnjhacking
- rej_ex https://twitter.com/rej_ex
- w0rmer https://twitter.com/0x686967
- ChiefCoolArrow https://twitter.com/ChiefCoolArrow
- Kelly https://twitter.com/kaoudis

# Precision Agriculture

- Every single farm is **connected.**

- 5G, LTE, 2G/3G, LoRa, WiFi, GPS, GPRS, WAAS, RTK, NTRIP

# Precision Ag Accuracy

# Accuracy

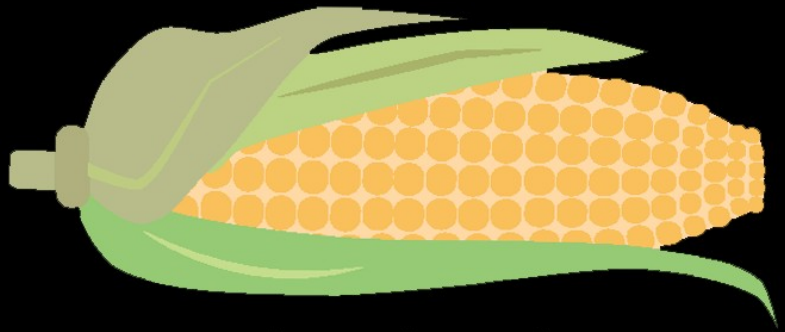
- https://www.flickr.com/photos/hindrik/50411142851/

# Accuracy

SF1

SF2

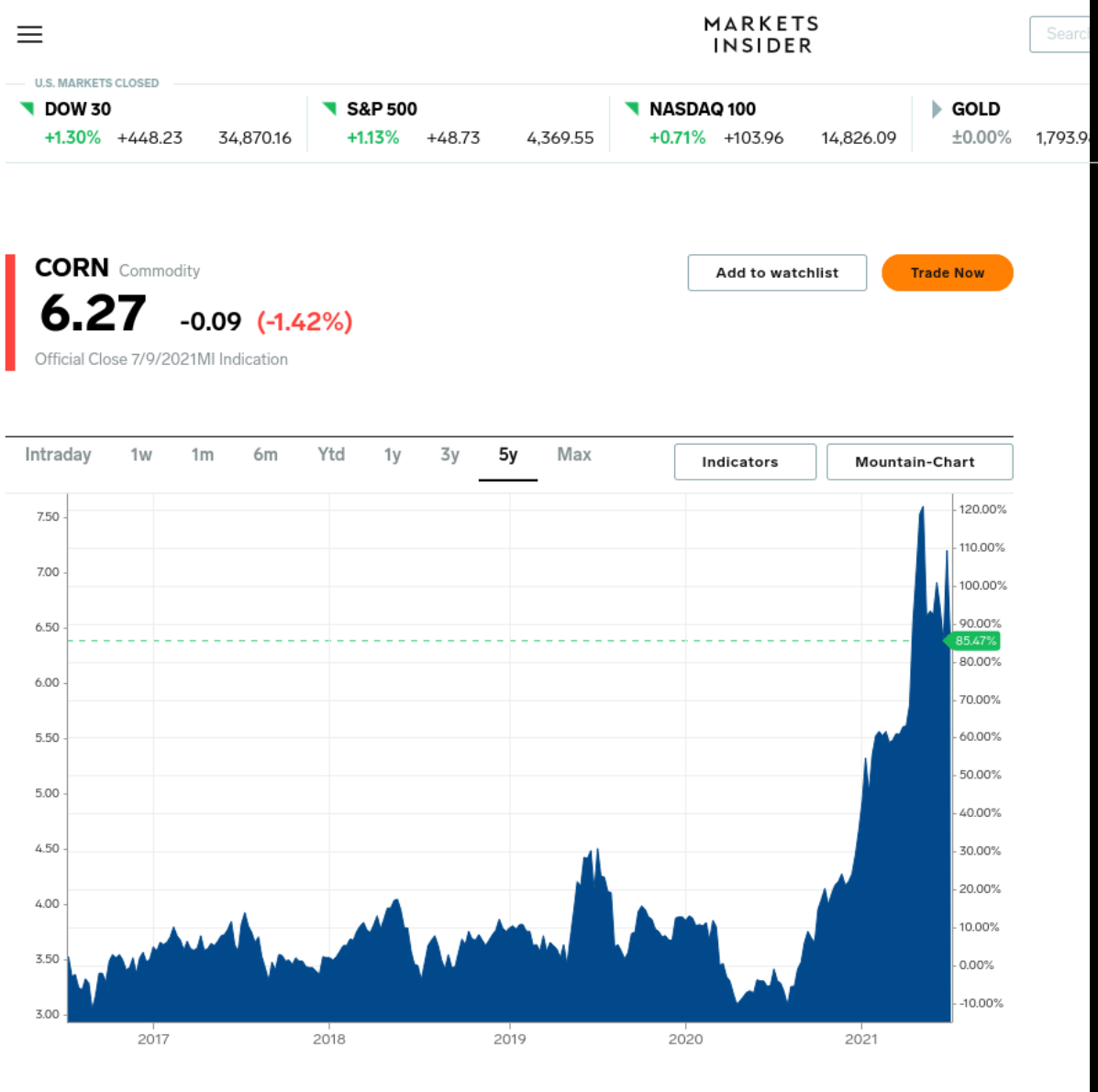
RTK



12 INCHES

https://www.vecteezy.com/vector-art/94697-free-ear-of-corn-vector

# What does the data do?



# "Trade Secrets"

- "Does sharing data with data analytic providers destroy its secrecy?"
- "{I think the answer is probably "no," provided sharing is done anonymously."
- https://www.aglaw.us/janzenaglaw/2015/9/30/is-farm-data-a-trade-secret

# Biofuel

# Other data usage

- Carbon credits (carbon offset market)

- Mandatory
- Voluntary

- *Shannon Sedgwick - Farmer turned Managing Director*

JOHN DEERE

# Display and CommandARM™ Simulator

Settings | Help | About | Troubleshooting | Last Update: June 30, 2021 | Logout

What would you like to simulate?

Start Simulation

**Machine**

Self-Propelled Forage Harvester

**Display**

GreenStar™ 3 CommandCenter™

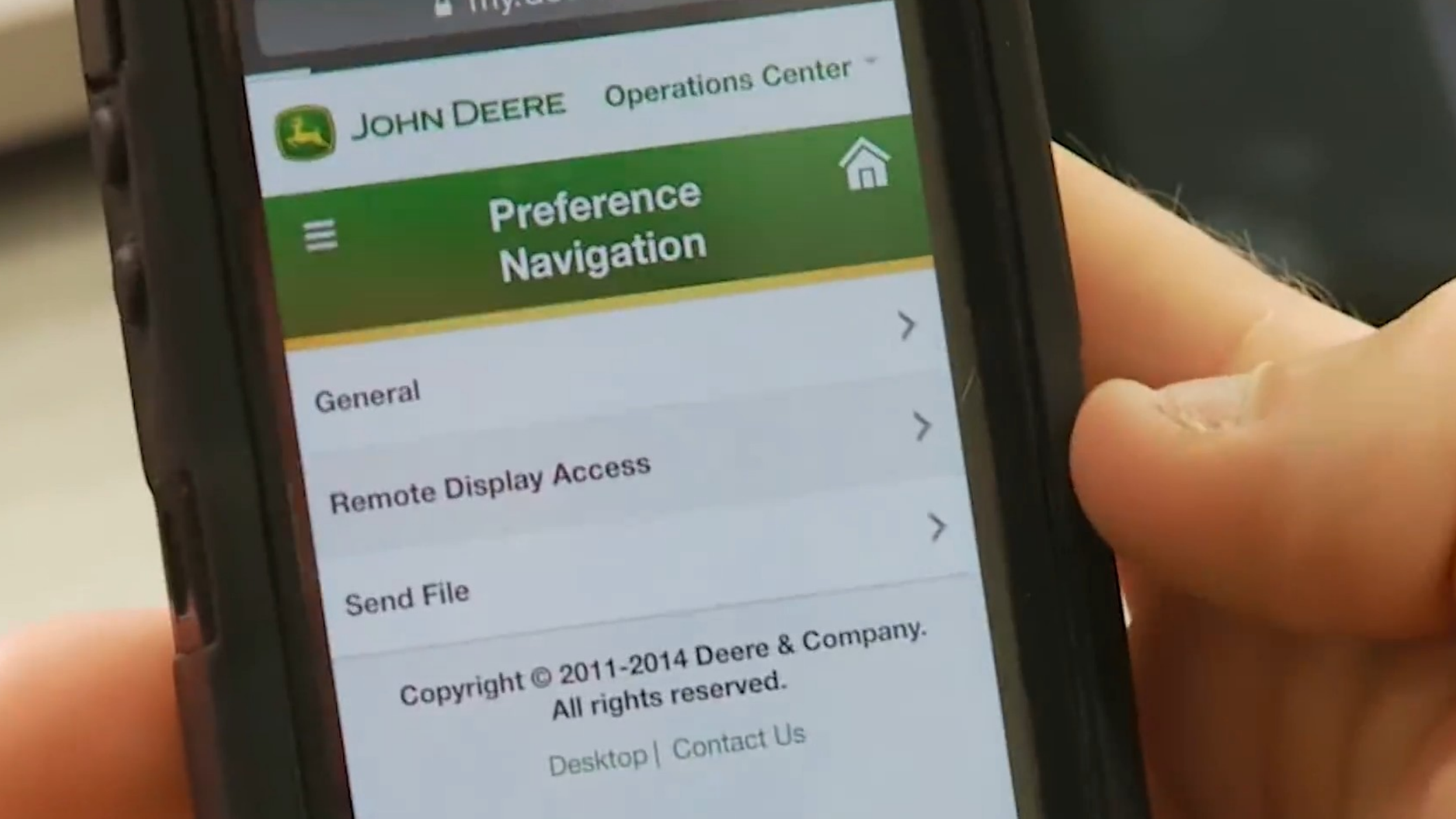
*Product models and options may not be available in all regions.*

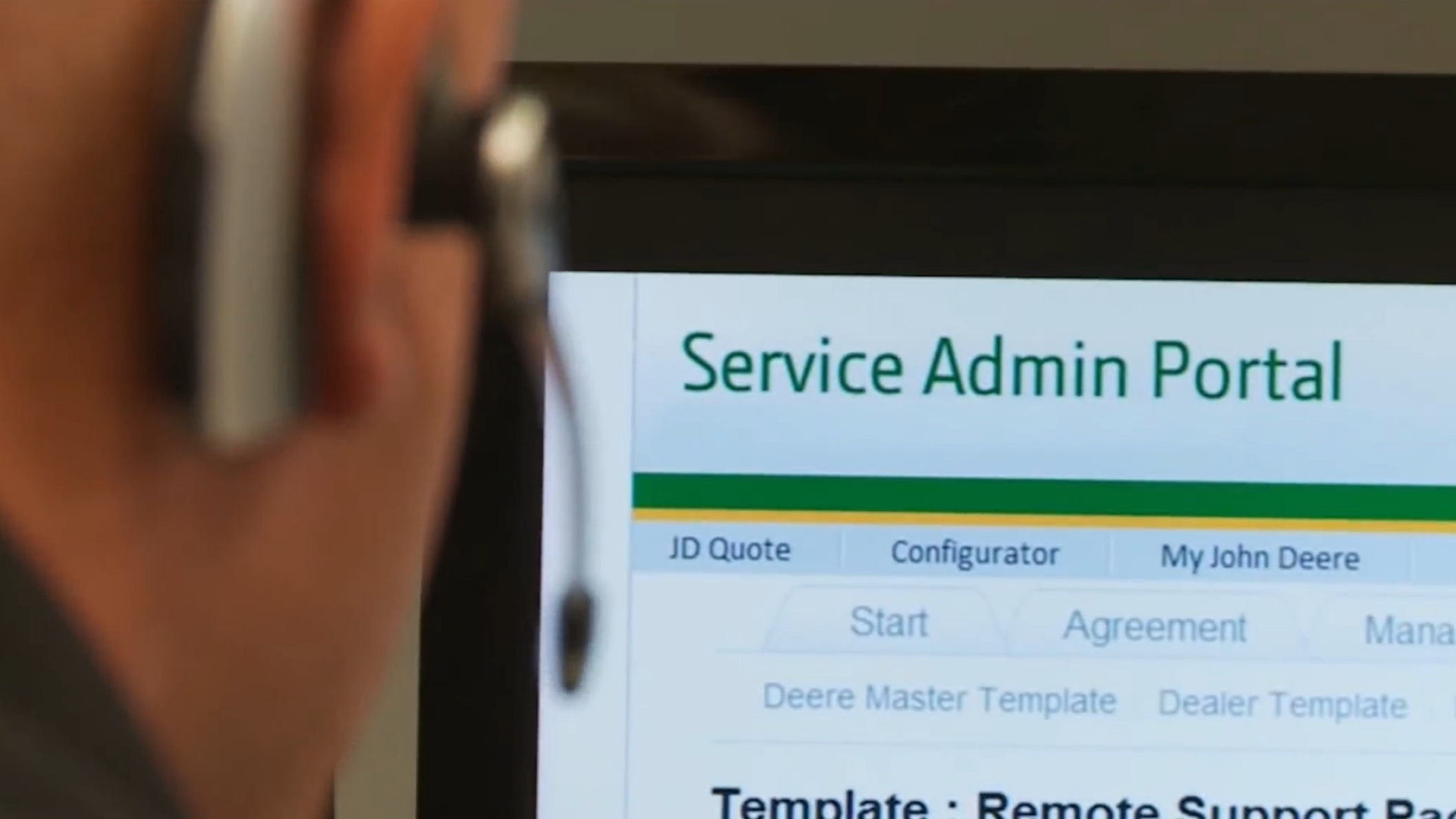
Expand all

## Machine

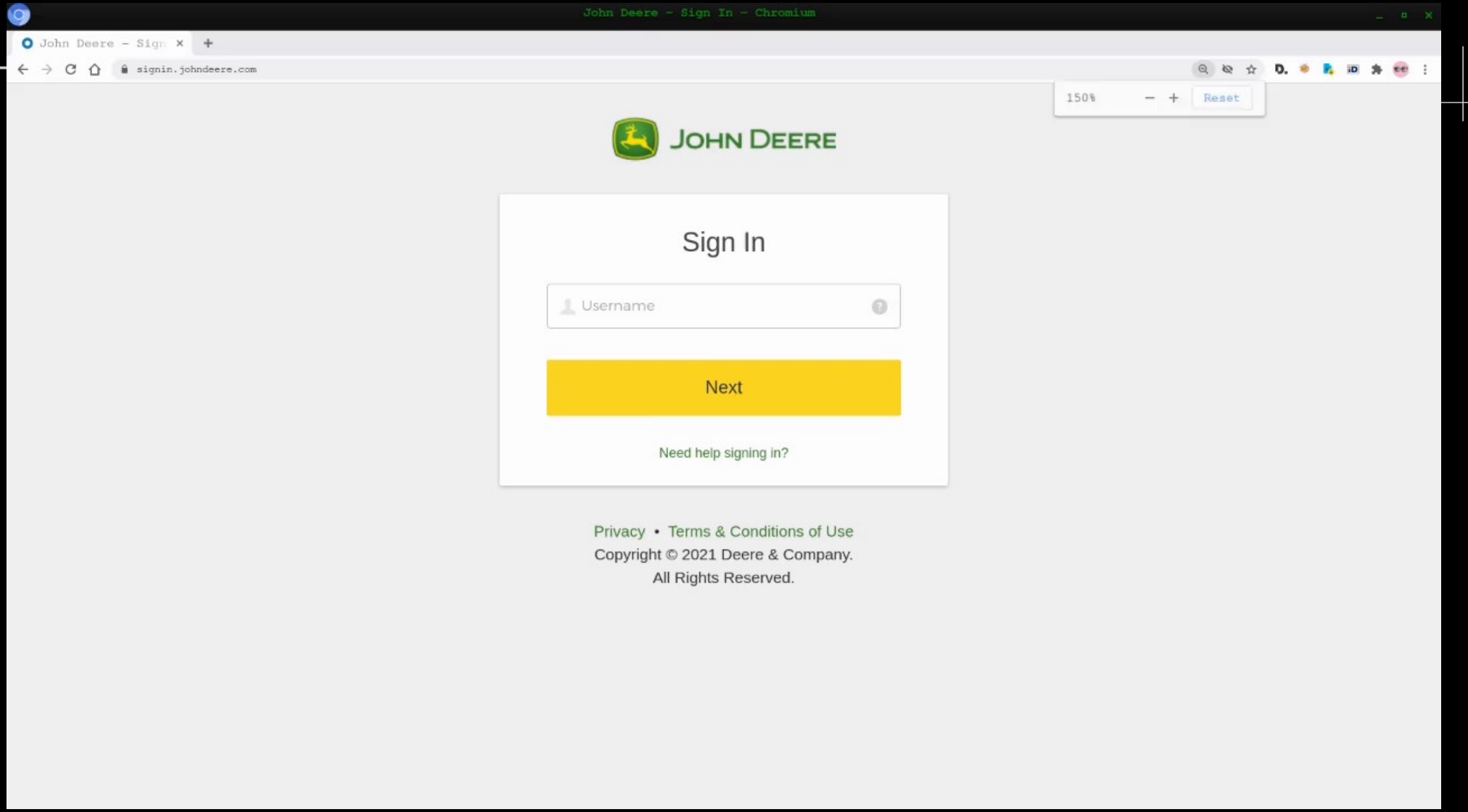
Self-Propelled Forage Harvester

# Internet of...


JOHN DEERE Operations Center
Preference Navigation
General
Remote Display Access
Send File
Copyright © 2011-2014 Deere & Company.
All rights reserved.
Desktop | Contact Us


Service Admin Portal
JD Quote
Configurator
My John Deere
Start
Agreement
Deere Master Template
Dealer Template

Dipping my feet in...


John Deere - Sign In - Chromium
John Deere - Sign
signin.johndeere.com
150%
Reset
JOHN DEERE
Sign In
Username
Next
Need help signing in?
Privacy • Terms & Conditions of Use
Copyright © 2021 Deere & Company.
All Rights Reserved.

MOTHERBOARD
TECH BY VICE

# Bugs Allowed Hackers to Dox John Deere Tractor Owners

A security researcher found two bugs that allowed him to find customers who had purchased John Deere tractors or equipment.

By Lorenzo Franceschi-Bicchierai

# “All” tractors

**Correction, April 22, 1:22 p.m. ET**: This article and headline have been corrected to clarify that not "all" owners of John Deere equipment were potentially affected by these vulnerabilities.

**wabafet**
@wabafet1

**wabafet** @wabafet1

I'm a passionate self taught researcher that likes to bug bounty hunt and program

**295** Following **200** Followers

Joined April 2021

hey bro how do i get ahold of vdp for deere got mad shit on them like 5 xss so far i can only imagine what the rest my toolkits gonan find in regards to p2 leaks

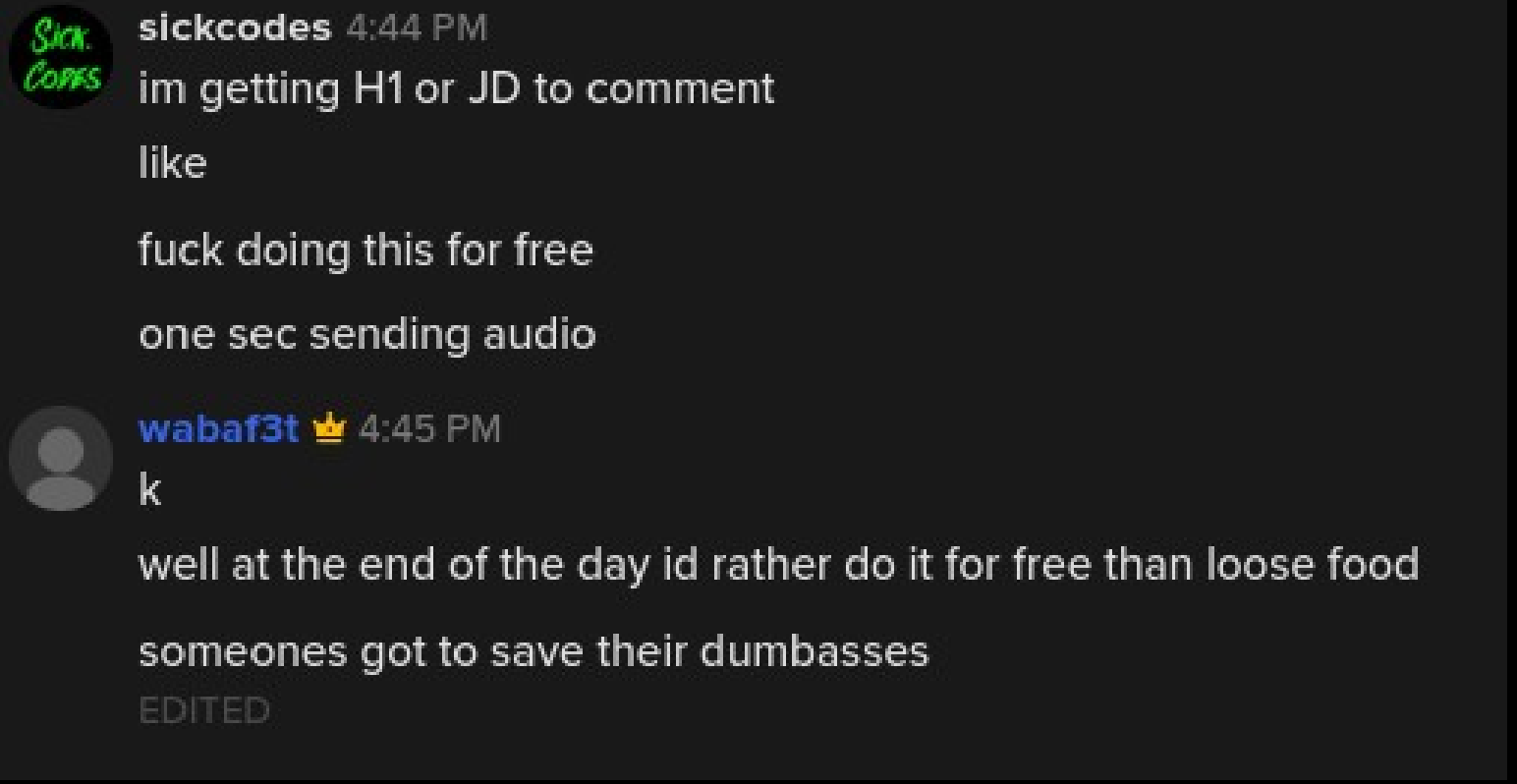
Apr 23, 2021, 1:59 PM

You accepted the request

Haha holy shit

You got signal?

Apr 23, 2021, 2:40 PM ✓


sickcodes 4:44 PM
im getting H1 or JD to comment
like
fuck doing this for free
one sec sending audio
wabaf3t 4:45 PM
k
well at the end of the day id rather do it for free than loose food
someones got to save their dumbasses
EDITED

John Deere @JohnDeere

Nothing runs like a Deere

**222** Following **196.2K** Followers

Joined January 2009

have a few pretty serious security bugs to report

1:38 AM ✓

i can be reached at wabafet@tutanota.com

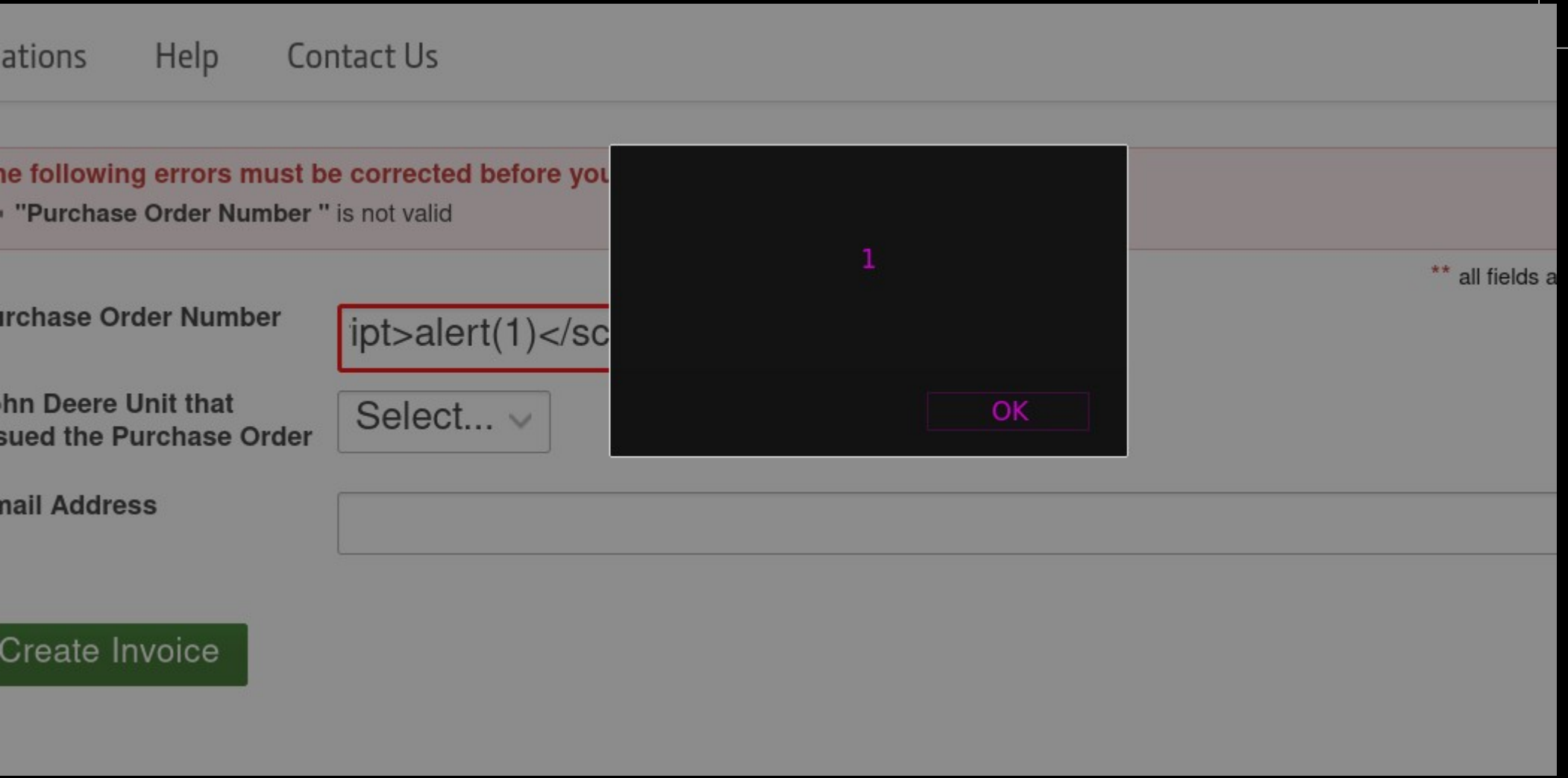
2:12 AM ✓

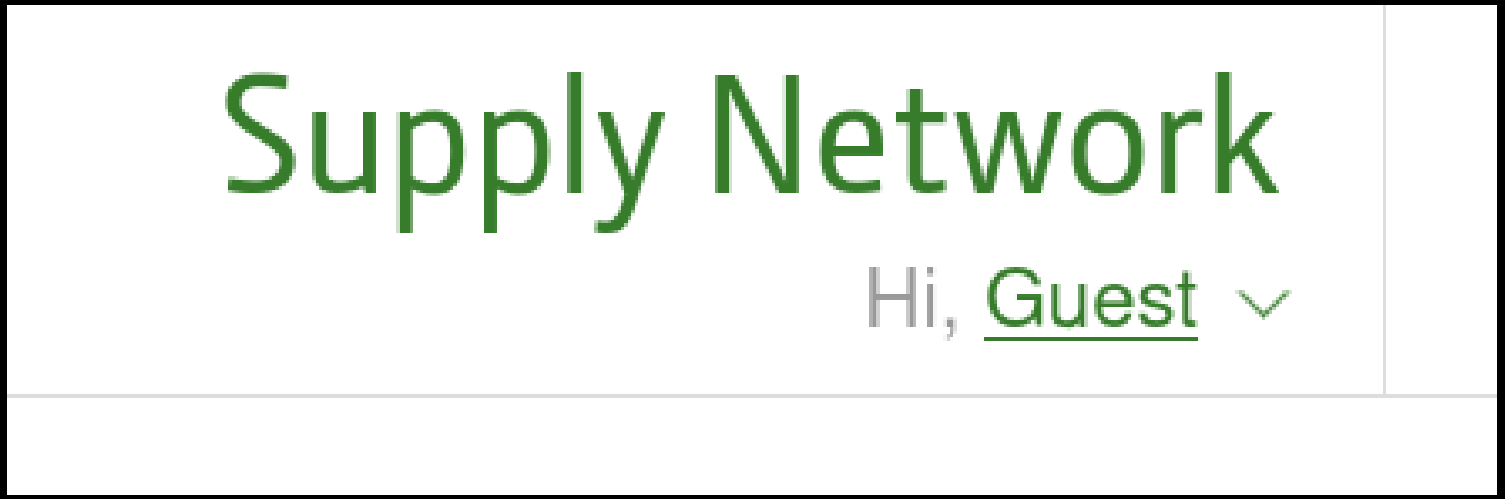
We encourage the ethical hacker community to report any possible vulnerability that is identified in our assets as we truly appreciate their work towards securing John Deere. Please submit vulnerabilities to us here: bit.ly/32LHxxO. We ensure safe harbor when vulnerabilities are reported in a good faith. At this time, do not have a bug bounty program or offer any monetary rewards for these submissions.

2:18 PM

ok i sent them in thank u for the reply if i may suggest can u add multiple bugs allowed  or something i had to submit u like 5 bugs in 1 secription field with no way to comment

2:24 PM ✓


ations
Help
Contact Us
he following errors must be corrected before you
"Purchase Order Number " is not valid
** all fields a
urchase Order Number
ipt>alert(1)</sc
ohn Deere Unit that
sued the Purchase Order
Select...
mail Address
Create Invoice
1
OK


Supply Network
Hi, Guest


Devl / Qual Supply Network
Hi, Guest

JOHN DEERE

e-Invoice | Applications | Help | Contact Us

- Create e-Invoice
- View e-Invoice Status
- Electronic Funds Transfer (EFT)
- Remit To Address Change

** all fields are required

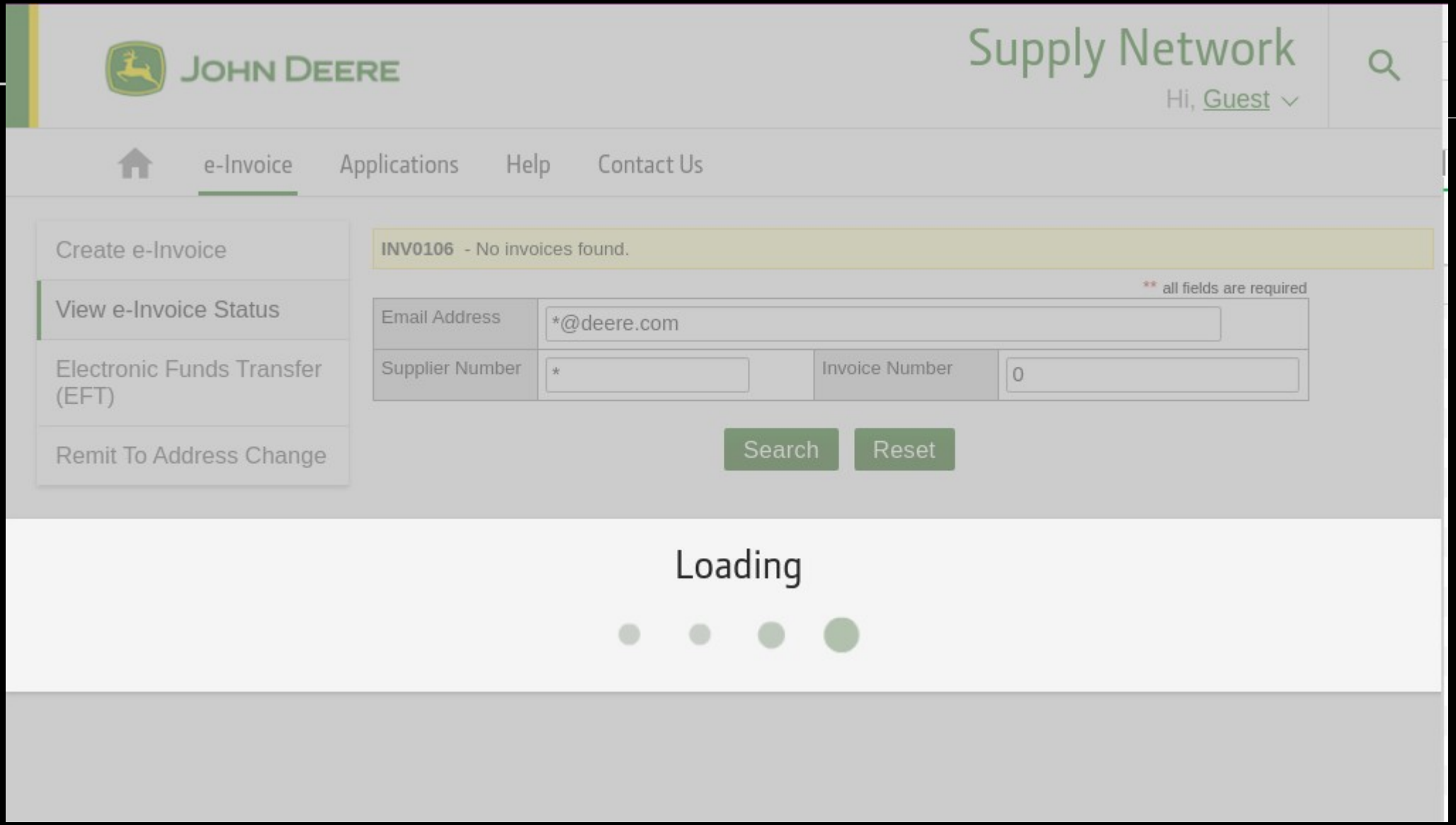
| | | | |
|---|---|---|---|
| Email Address | | | |
| Supplier Number | | Invoice Number | |

Search Reset

## New Functionality!

Now, you just have to provide a PO number and E-Invoice will filter and display the units related to who wrote the PO.

Got it!


JOHN DEERE
Supply Network
Hi, Guest
e-Invoice
Applications
Help
Contact Us
Create e-Invoice
View e-Invoice Status
Electronic Funds Transfer (EFT)
Remit To Address Change
INV0106 - No invoices found.
** all fields are required
Email Address
*@deere.com
Supplier Number
*
Invoice Number
0
Search
Reset
Loading

JOHN DEERE

# Supply Network

Hi, Guest

e-Invoice | Applications | Help | Contact Us

- Create e-Invoice
- View e-Invoice Status
- Electronic Funds Transfer (EFT)
- Remit To Address Change

**INV0106** - No invoices found.

** all field

| Email Address | *@deere.com | | |
|---|---|---|---|
| Supplier Number | * | Invoice Number | 0 |

Search Reset

# We're sorry, there was an application error.

**Please contact the Help Desk by phone or email with the Diagnostic Information below.**

You may want to print this page as it has important information about the error.

Go back to the page I was viewing

## Diagnostic Information

| | |
|---|---|
| **User ID** | |
| **Server Time** | 2021-04-25 20:10:33.881 |
| **Application Name** | e-Invoice |
| **Application URL** | /invoice/servlet/com.deere.u90242.invoice.view.servlets.SelectPOServlet |
| **Error Message** | Offending query is: SELECT COUNT(PO_NUM) TOTAL FROM (SELECT DISTINCT PO_NUM FROM DJDBP01.PURCH_HRZN_PO_DTL WHERE PO_NUM = '' UNION ALL SELECT DISTINCT PO_NUM FROM DJDBP01.SM_IND_ORD_HDR WHERE PO_NUM = '' ) |

**Sign in to Access My JDSN**

**Already Have a User ID?**

Sign In

**No User ID?**

How to Obtain Access?

**JDSN Applications**

- Applications by Name
- How Do I...

Filter Results:

| Application Name | Functional Area |
|---|---|
| Achieving Excellence | Supplier Quality & Performance |
| Change Request | EPDP/SCI/Collab |
| Compliance Information Collection (CIC) | Compliance |
| Credit Memo | Order Management |
| Delivery Receipts | Order Management |
| Demand Report | Order Management |
| e-Invoice | Order Management |
| EOD Commercial Invoice | Global Trade Management |
| EOD Export ESO System | Global Trade Management |
| EOD Hazardous Material Form | Global Trade Management |
| EOD Ship Notice | Global Trade Management |
| Forgot My Password | Other |
| Fulfill Email Preferences | Order Management |
| Indirect Open Orders | Order Management |
| Invoice and Payment Status | Order Management |
| Invoice Attachments | Order Management |
| JD Color Standards | Other |
| JD CROP | Cost Management |
| JD Supplier Warranty | Supplier Quality & Performance |
| JDSN Collaboration | EPDP/SCI/Collab |
| Manufacturing Critical-path Time (MCT) | Order Management |
| Non-Conformance Corrective Action (NCCA) | Other |
| North American Freight Invoices | Logistics |
| Open Triggers | Order Management |
| Shipment Tracking | Logistics |
| Standard Shipping Label | Global Trade Management |
| Supplier Capability Planning | Order Management |
| Supplier Contacts | Supplier Information |
| Supplier Diversity | Other |
| Supplier Education Program | Other |

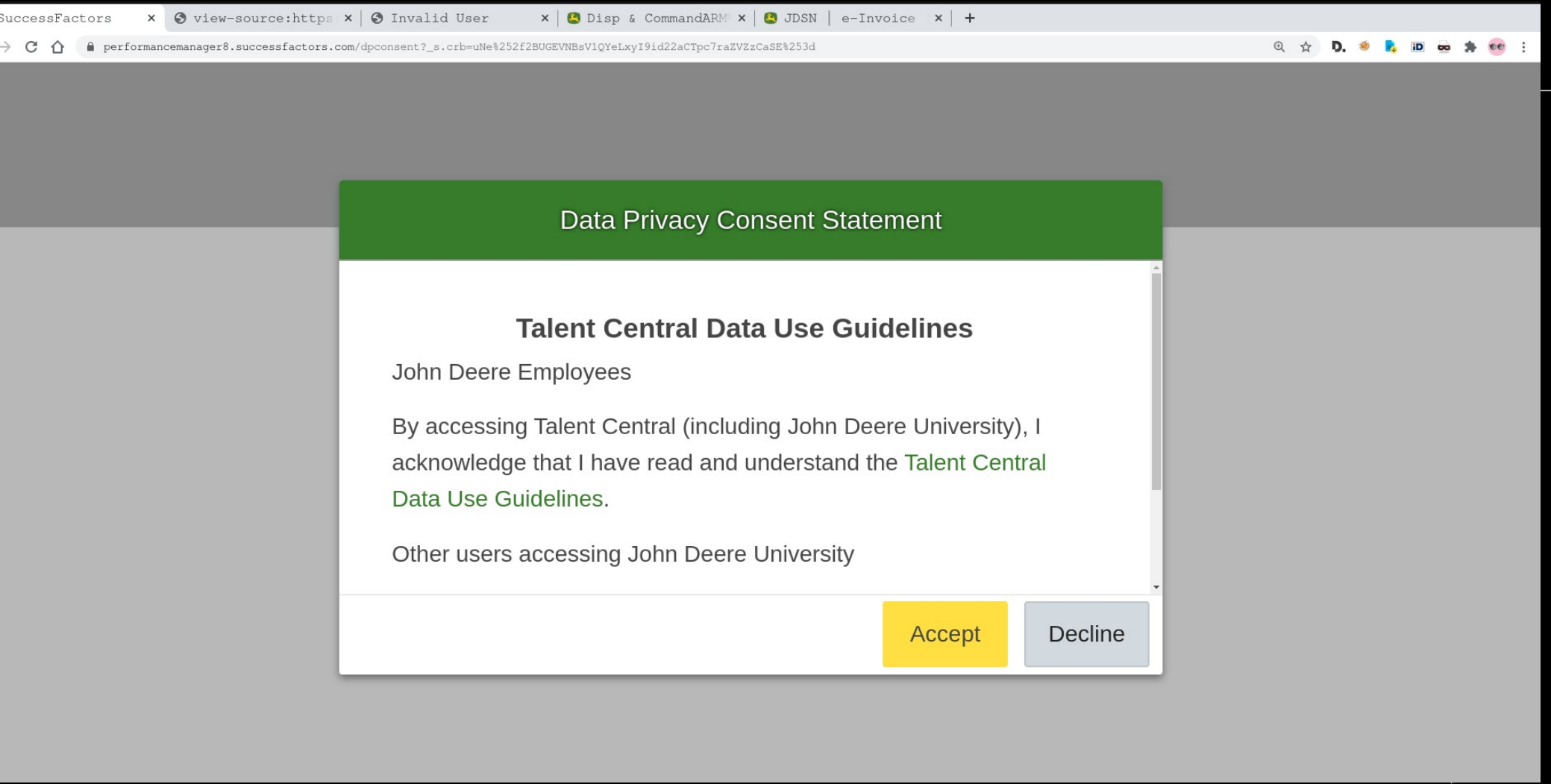
JOHN DEERE

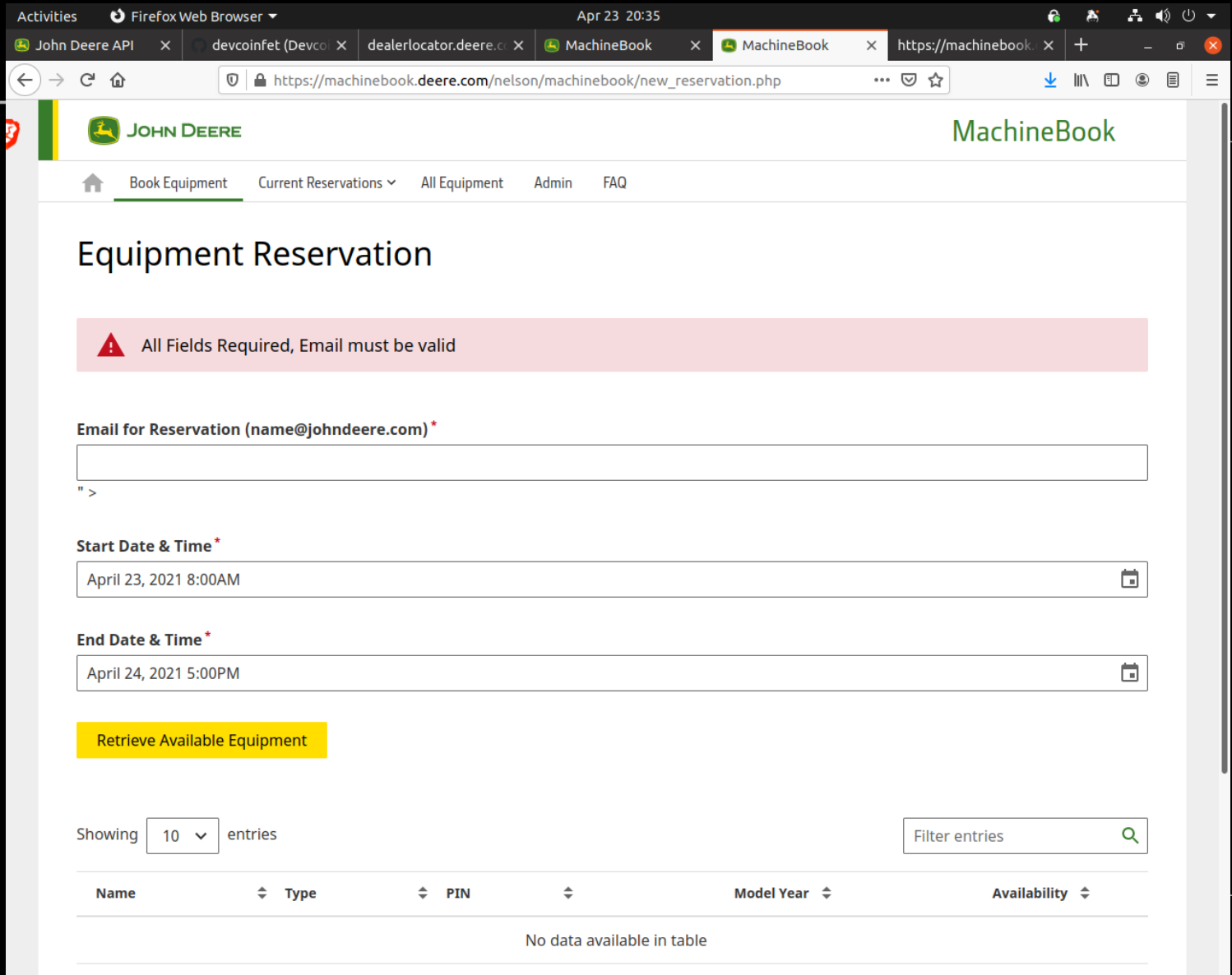
LMSSO

Welcome Sick Codes | Logout

## Application Error

| | |
|---|---|
| **Message:** | java.io.FileNotFoundException: SRVE0190E: File not found: /P/ |
| null | |


SuccessFactors
view-source:https
Invalid User
Disp & CommandARM
JDSN
e-Invoice
performancemanager8.successfactors.com/dpconsent?_s.crb=uNe%252f2BUGEVNBsV1QYeLxyI9id22aCTpc7raZVZzCaSE%253d
Data Privacy Consent Statement
Talent Central Data Use Guidelines
John Deere Employees
By accessing Talent Central (including John Deere University), I acknowledge that I have read and understand the Talent Central Data Use Guidelines.
Other users accessing John Deere University
Accept
Decline


Activities
Firefox Web Browser
Apr 23 20:35
John Deere API
devcoinfet (Devco
dealerlocator.deere.c
MachineBook
MachineBook
https://machinebook.
https://machinebook.deere.com/nelson/machinebook/new_reservation.php
JOHN DEERE
MachineBook
Book Equipment
Current Reservations
All Equipment
Admin
FAQ
Equipment Reservation
All Fields Required, Email must be valid
Email for Reservation (name@johndeere.com) *
" >
Start Date & Time *
April 23, 2021 8:00AM
End Date & Time *
April 24, 2021 5:00PM
Retrieve Available Equipment
Showing 10 entries
Filter entries
Name
Type
PIN
Model Year
Availability
No data available in table

JOHN DEERE

MachineBook

Book Equipment | Current Reservations | All Equipment | Admin | FAQ

# All Equipment

Showing 100 e

Name

| | | | | |
|---|---|---|---|---|
| 8RX 370 (F9a) | | | lable | Details |
| 9RX 490 (F11) | | | lable | Details |
| 9RT 570 (F11) | | | lable | Details |
| 410R | | | lable | Details |
| DB60 36R20 (Gaines | | | lable | Details |
| 612R (D8) | Self-Propelled Sprayer | [redacted] | Unavailable | Details |

Showing 101 to 106 of 106 entries

Previous 1 2 Next

## Equipment Details

DB60[redacted](PIN:[redacted])

Equipment Type: Implement - Planter

Model Year: MY22

Additional Notes: [redacted]

Requires additional equipment

Upcoming Schedule:

| Reserved By | Start | End |
|---|---|---|
| [redacted]johndeere.com | 8:00am on April 27th | 5:00pm on April 28th |

```
[20:58:04] [INFO] fetching columns for table 'reservations' in database 'machinebook'
[20:58:05] [INFO] fetching entries for table 'reservations' in database 'machinebook'
Database: machinebook
Table: reservations
[810 entries]
+-----+------------+------------+--------------+----------------------------------+---------------------+------
| id  | machine_id | reserve_id | implement_id | name                             | end                 | start
+-----+------------+------------+--------------+----------------------------------+---------------------+------
[20:58:07] [WARNING] console output will be trimmed to last 256 rows due to large table size
| 618 | 12         |            | NULL         |                ndeere.com        | 2021-03-19 17:00:00 | 2021-0
| 619 | 114        |            | NULL         |           m@johndeere.com        | 2021-03-18 17:00:00 | 2021-0
| 620 | 7          |            | NULL         |            hndeere.com           | 2021-03-19 12:00:00 | 2021-0
| 621 | 114        |            | NULL         |           m@johndeere.com        | 2021-03-19 13:00:00 | 2021-0
| 622 | 21         |            | NULL         |                ndeere.com        | 2021-03-19 12:00:00 | 2021-0
| 623 | 88         |            | NULL         |           m@johndeere.com        | 2021-03-19 17:00:00 | 2021-0
| 624 | 27         |            | NULL         |                ndeere.com        | 2021-03-19 15:00:00 | 2021-0
| 625 | 99         |            | NULL         |           @johndeere.com         | 2021-03-26 16:00:00 | 2021-0
| 626 | 6          |            | NULL         |           m@johndeere.com        | 2021-03-22 17:00:00 | 2021-0
| 627 | 30         |            | 49           |                ndeere.com        | 2021-03-22 12:00:00 | 2021-0
| 628 | 12         |            | NULL         |                ndeere.com        | 2021-03-22 17:00:00 | 2021-0
| 629 | 90         |            | NULL         |                deere.com         | 2021-03-23 17:00:00 | 2021-0
| 630 | 112        |            | 50           |            hndeere.com           | 2021-03-22 17:00:00 | 2021-0
| 631 | 104        |            | NULL         |                deere.com         | 2021-03-23 17:00:00 | 2021-0
| 632 | 104        |            | NULL         |                deere.com         | 2021-03-22 17:00:00 | 2021-0
| 633 | 111        |            | NULL         |            hndeere.com           | 2021-03-23 17:00:00 | 2021-0
| 634 | 86         |            | NULL         |           @JohnDeere.com         | 2021-03-25 17:00:00 | 2021-0
| 635 | 21         |            | 54           |           ohnDeere.com           | 2021-03-22 17:00:00 | 2021-0
```

```
1  ************************************
2  *       Edge Server Files          *
3  ************************************
4
5  This directory (where this ReadMe.txt file is located) and its
   subdirectories contain
6  PRPC static content files generated for the following Rule
   Application instance:
7
8  Rule Application Name: DeereSSOSAML
9  Rule Application Version: 01.01.01
10
11 For more details consult PDN and look for KB article entitled :
   "How to deploy static content to an Edge Server".
```

# rej_ex & john jackson's CVE

CVE List▾ CNAs▾ WGs▾ Board▾ About▾ News & Blog▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

**TOTAL CVE Records: 156599**

HOME > CVE > CVE-2021-27653

Printer-Friendly View

| CVE-ID | |
|---|---|
| **CVE-2021-27653** | Learn more at National Vulnerability Database (NVD)<br>• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information |

**Description**

Misconfiguration of the Pega Chat Access Group portal in Pega platform 7.4.0 - 8.5.x could lead to unintended data exposure.

**References**

**Note:** References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

# rej_ex & john jackson's CVE

- https://robertwillishacking.com/cve-2021-27653-march-2021/

| | | |
|---|---|---|
| **NIST:** NVD | **Base Score:** 4.9 MEDIUM | **Vector:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N |
| **CNA:** Pegasystems Inc. | **Base Score:** 6.6 MEDIUM | **Vector:** CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |

# Extract EdgeServer Files

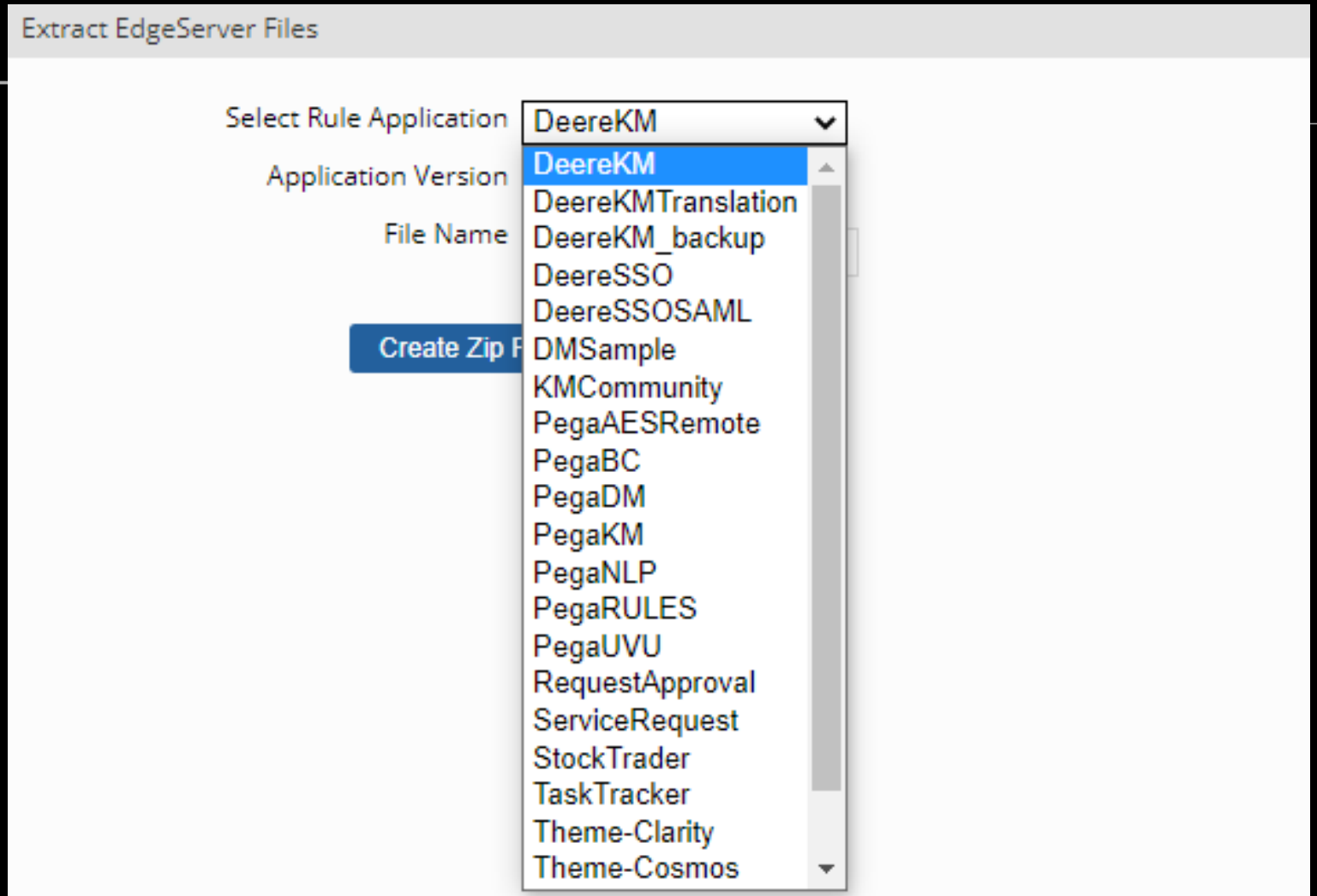
Select Rule Application: DeereKM

Application Version: 01.01.01

File Name:

Create Zip File

Close


Extract EdgeServer Files
Select Rule Application
DeereKM
Application Version
File Name
Create Zip F
DeereKM
DeereKMTranslation
DeereKM_backup
DeereSSO
DeereSSOSAML
DMSample
KMCommunity
PegaAESRemote
PegaBC
PegaDM
PegaKM
PegaNLP
PegaRULES
PegaUVU
RequestApproval
ServiceRequest
StockTrader
TaskTracker
Theme-Clarity
Theme-Cosmos

```
1  ************************************
2  *       Edge Server Files          *
3  ************************************
4
5  This directory (where this ReadMe.txt file is located) and its
   subdirectories contain
6  PRPC static content files generated for the following Rule
   Application instance:
7
8  Rule Application Name: DeereSSOSAML
9  Rule Application Version: 01.01.01
10
11 For more details consult PDN and look for KB article entitled :
   "How to deploy static content to an Edge Server".
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<pagedata>
   <pxUpdateSystemID>[redacted]</pxUpdateSystemID>
   <pyClassName/>
   <pxUpdateDateTime>20141201T091133.492 GMT</pxUpdateDateTime>
   <pxFrom>PortalServer</pxFrom>
   <pxMoveImportOperName>[redacted]</pxMoveImportOperName>
   <pxUpdateOpName>Administrator</pxUpdateOpName>
   <pyWindowTitle/>
   <pxUpdateOperator>Administrator@pega.com</pxUpdateOperator>
   <pyHasCustomFields/>
   <pyUsage/>
   <pxMoveFromSystem/>
   <pxCreateDateTime>20110323T053818.659 GMT</pxCreateDateTime>
   <pyRuleSet/>
   <pyDescription/>
   <pyPassword>[redacted]</pyPassword>
   <pyHistoryObject/>
   <pyTemplateDataField/>
   <pxMoveImportOperId>[redacted]</pxMoveImportOperId>
   <pxInsName>PORTALSERVER</pxInsName>
   <pxSaveDateTime>20161227T041629.496 GMT</pxSaveDateTime>
   <pyFormPost/>
   <pyIsTagged>true</pyIsTagged>
   <pyAccessGroup>PRPC:PortalUsers</pyAccessGroup>
   <pyTemplateDefault/>
   <pyTemporaryObject/>
   <pzInsKey>DATA-ADMIN-APPID PORTALSERVER</pzInsKey>
   <pyTemplate/>
   <pyTimeDifferenceShadow>[redacted]</pyTimeDifferenceShadow>
   <pxMoveImportDateTime>20121218T134807.752 GMT</pxMoveImportDateTime>
   <pxObjClass>Data-Admin-AppID</pxObjClass>
   <pxTimeDifference>[redacted]</pxTimeDifference>
   <pxCreateOperator>Administrator@[redacted].com</pxCreateOperator>
   <pyTemplateInputBox/>
   <pySPRuleSetName/>
   <pyReloadForm>true</pyReloadForm>
   <pyDeletedObject/>
   <pxCreateSystemID>pega</pxCreateSystemID>
   <pxLimitedAccess>Dev</pxLimitedAccess>
   <pxCommitDateTime>20180214T153521.000 GMT</pxCommitDateTime>
   <pyLabel>PortalServer</pyLabel>
   <pzOriginalInstanceKey>DATA-ADMIN-APPID PORTALSERVER</pzOriginalInstanceKey>
   <pxCreateOpName>Administrator</pxCreateOpName>
   <pyRuleSetName>Pega-ProcessCommander</pyRuleSetName>
   <pzStatus>valid</pzStatus>
   <pxWarnings REPEATINGTYPE="PageList"/>
 </pagedata>
```

<pxUpdateOpName>Administrator</pxUpdateOpName>
<pyWindowTitle/>
<pxUpdateOperator>Administrator@pega.com</pxUpdateOperator>
<pyHasCustomFields/>
<pyUsage/>
<pxMoveFromSystem/>
<pxCreateDateTime>20110323T053818.659 GMT</pxCreateDateTime>
<pyRuleSet/>
<pyDescription/>
<pyPassword>[redacted]</pyPassword>
<pyHistoryObject/>
<pyTemplateDataField/>
<pxMoveImportOperId>[redacted]</pxMoveImportOperId>
<pxInsName>PORTALSERVER</pxInsName>
<pxSaveDateTime>20161227T041629.496 GMT</pxSaveDateTime>
<pyFormPost/>
<pyIsTagged>true</pyIsTagged>
<pyAccessGroup>PRPC:PortalUsers</pyAccessGroup>
<pyTemplateDefault/>
<pyTemporaryObject/>
<pzInsKey>DATA-ADMIN-APPID PORTALSERVER</pzInsKey>
<pyTemplate/>
<pyTimeDifferenceShadow>[redacted]</pyTimeDifferenceShadow>
<pxMoveImportDateTime>20121218T134807.752 GMT</pxMoveImportDateTime>
<pxObjClass>Data-Admin-AppID</pxObjClass>
<pxTimeDifference>[redacted]</pxTimeDifference>
<pxCreateOperator>Administrator@[redacted].com</pxCreateOperator>
<pyTemplateInputBox/>

# Security Audit Log

Filtered by: .pxCreateDateTime

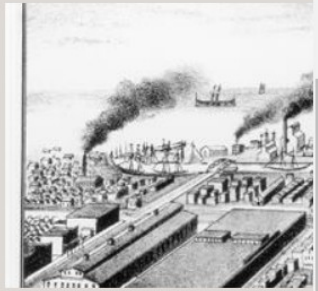
Displaying 50 records

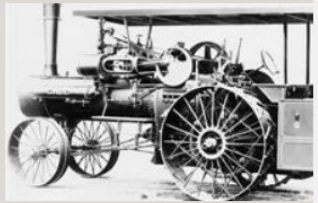
| Create Date/Time ↓ | Remote IP Address | Remote Host | User Id | Message | Browser(User-Agent) |
|---|---|---|---|---|---|
| 4/23/2021 11:03 PM | [redacted] | | | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64) AppleW |
| 4/23/2021 11:02 PM | | | | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64) AppleW |
| 4/23/2021 10:56 PM | | | pega.com | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64) AppleW |
| 4/23/2021 10:55 PM | | | | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64) AppleW |
| 4/23/2021 10:16 PM | | | @pega.com | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64; rv:78.0) |
| 4/23/2021 10:16 PM | | | @pega.com | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64; rv:78.0) |
| 4/23/2021 10:15 PM | | | @pega.com | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64; rv:78.0) |
| 4/23/2021 10:15 PM | | | @pega.com | The information you entered was not recognized. | Mozilla/5.0 (X11; Linux x86_64; rv:78.0) |

```
<pyIDPIdentifier>http://www.okta.com/[redacted]7</pyIDPIdentifier>
<pyIsSigningDisabled>false</pyIsSigningDisabled>
<pySPIdentifier>https://kms.deere.co[redacted]</pySPIdentifier>
<pyIDPSigningCertificateExpiry>Tue Aug 03 02:41:26 CDT 2027</pyIDPSigningCertificateExpiry>
<pyOriginalDecryptionPasswordRUF />
<pyIDPCertificateToVerifySignature />
<pyOriginalSignaturePassword>[redacted]
pyOriginalSignaturePassword>
<pyOriginalSignaturePasswordRUF />
<pyOriginalDecryptionUser>prod</pyOriginalDecryptionUser>
<pyOriginalDecryptionPassword>[redacted]
pyOriginalDecryptionPassword>
<pyIDPSigningCertificateAlias>EMAILADDRESS=info@okta.com, CN=johndeerecustomer,
OU=SSOProvider, O=Okta, L=San Francisco, ST=California, C=US</pyIDPSigningCertificateAlias>
<pyOriginalDecryptionPasswordSource>Direct</pyOriginalDecryptionPasswordSource>
<pyIsImportMetadataSuccess>true</pyIsImportMetadataSuccess>
<pyTemporaryObject />
<pzInsKey />
<pyOriginalIDPSigningCertificateAlias>emailaddress=info@okta.com, cn=[redacted]
ou=ssoprovider, o=okta, l=san francisco, st=california, c=us</
pyOriginalIDPSigningCertificateAlias>
<pySingleSignOnServiceURL>https://signin.johndeere.com/app/johndeere_saml_1/
[redacted]</pySingleSignOnServiceURL>
<pySPSigningCertificateExpiry>Mon Sep 10 07:39:38 CDT 2029</pySPSigningCertificateExpiry>
<pyDecryptionPassword>[redacted]</pyDecryptionPassword>
```

# CASE IH + NEW HOLLAND

PRODUCTS | COMPANY | CONNECT WITH US | SERVICE & SUPPORT | TOOLS & RESOURCES



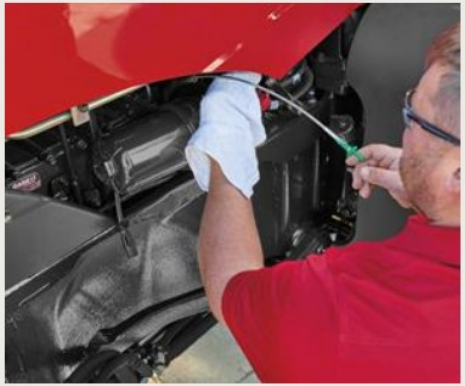


https://www.caseih.com/northamerica/en-us/products/tractors/afs-connect-magnum-series

MAINTENANCE & UPTIME

# Remote Support and Resources to Maximize Productivity

Whether you are three miles or 300 miles away, you can get the support you need from your knowledgeable Case IH dealer. New features allow them to better support you and your fleet remotely — and in real time.

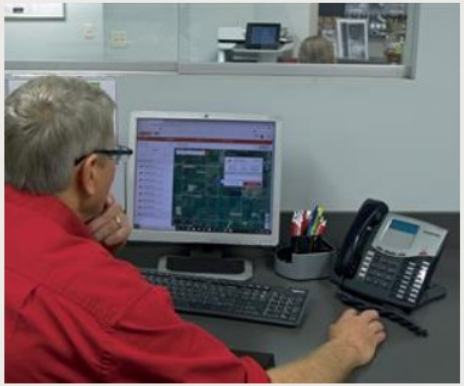


**Ground-level Fluid Checks**

Ground-level fluid checks from a single location near the cab entry help you to stay on top of maintenance as quickly as possible.

**600-hour Oil Change Intervals**

Stay in the field longer with Industry leading oil service change intervals.



**Remote Dealer Support**

From setting up your new AFS Connect Magnum tractor to diagnosing machine codes, your dealer is just a call away to provide you remote support.

**Information at Your Fingertips**

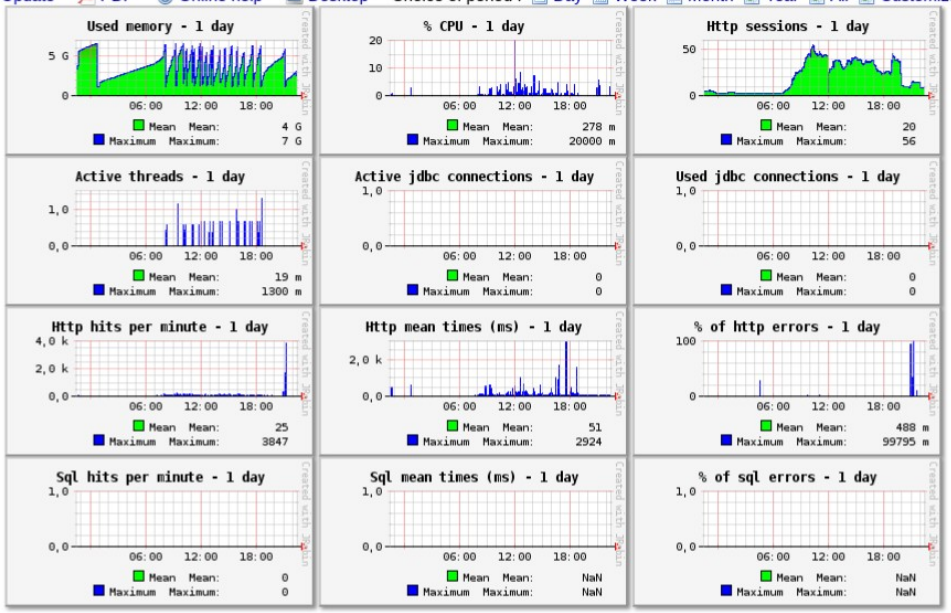
MyCaseIH.com is your all-new destination for product support, including free operators manual downloads, AFS training videos, how-to tutorials and maintenance tips.

A new version of JavaMelody is available (1.87.0 instead of 1.72.0, see Release Notes)

Donate

## Statistics of JavaMelody monitoring taken at 4/28/21 10:24 PM on _MIBHFCATC03 (nh360)

Update PDF Online help Desktop Choice of period : Day Week Month Year All Customized




Other cha

## Statistics http - 1 day

| Request | % of cumulative time | Hits | Mean time (ms) | Max time (ms) | Standard deviation | % of cumulative cpu time | Mean cpu time (ms) | % of system error | Mean size (Kb) |
|---|---|---|---|---|---|---|---|---|---|
| http global | 100 | 37,739 | 47 | 84,828 | 676 | 100 | 15 | 26.13 | |
| http warning | 8 | 142 | 1,095 | 13,111 | 2,183 | 5 | 210 | 0.00 | |
| http severe | 28 | 115 | 4,451 | 84,828 | 10,788 | 4 | 240 | 0.00 | 2 |

28 hits/min on 572 requests Details

| Request | % of cumulative time | Hits | Mean time (ms) | Max time (ms) | Standard deviation | % of cumulative cpu time | Mean cpu time (ms) | % of system error | Mean size (Kb) |
|---|---|---|---|---|---|---|---|---|---|
| /ajax/repository/standardResource/sendMinutesPreviewEmail ajax POST | 14 | 7 | 36,895 | 84,828 | 26,553 | 1 | 847 | 0.00 | |
| /ajax/repository/directMessage/refresh ajax POST | 10 | 3,355 | 56 | 4,063 | 117 | 21 | 36 | 0.00 | |
| /pages/portal GET | 4 | 206 | 410 | 3,932 | 413 | 9 | 275 | 0.00 | |
| /pages/user/userManagerEdit POST | 4 | 64 | 1,119 | 4,383 | 2,366 | 1 | 142 | 0.00 | |
| /ajax/repository/strategicPlanResource/loadItem ajax POST | 3 | 191 | 331 | 1,227 | 260 | 6 | 186 | 0.00 | |
| /ajax/dynamicSelect/responsibleSelectUser ajax GET | 3 | 450 | 135 | 289 | 205 | 6 | 78 | 0.00 | |
| /pages/pm/cc/receipt/pmCcMediaReceiptManagerEdit POST | 1 | 22 | 1,445 | 7,678 | 4,182 | 0 | 112 | 0.00 | |
| /pages/account/tempPassword POST | 1 | 14 | 2,265 | 7,129 | 3,088 | 0 | 66 | 0.00 | |
| /pages/actionPlan/actionPlanItemEdit POST | 1 | 10 | 3,094 | 5,888 | 4,419 | 0 | 97 | 0.00 | |
| /ajax/i18n/resources/1 GET | 1 | 55 | 497 | 3,220 | 683 | 0 | 54 | 0.00 | 5 |
| /ajax/repository/standardResource/getModuleTotal ajax POST | 1 | 26 | 1,030 | 10,138 | 2,212 | 1 | 325 | 0.00 | |
| /css/ace.min.css GET | 1 | 307 | 85 | 2,839 | 327 | 0 | 4 | 0.00 | |
| /jqGrid/jquery.jqGrid.js GET | 1 | 184 | 139 | 3,297 | 438 | 0 | 7 | 0.00 | |

Return Update

## Details session 6

| Session id | Last access | Age | Expiration | Number of attributes | Serializable | Serializable size (b) | IP address | Country | Browser | OS | Invalidate |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [redacted] | 00:00:18 | 01:10:17 | 5/4/21 8:49 AM | 5 | no | -1 | 200.218.138.137 | | | | |

## Attributes

| Name | Type | Serializable | Serializable size (b) | Content |
|---|---|---|---|---|
| javamelody.sessionActivation | net.bull.javamelody.SessionListener | yes | 75 | SessionListener[sessionCount=11] |
| javamelody.userAgent | java.lang.String | yes | 137 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM like Gecko) Chrome/90.0.4430.72 Safari/537.36 Edg/90.0.818.41 |
| javamelody.remoteAddr | java.lang.String | yes | 22 | 200.218.138.137 |
| javamelody.country | java.lang.String | yes | 9 | BR |
| DirectMessageHandler-Object | br.com.usecase.cnh.view.directmessage.DirectMessageHandler | no | -1 | br.com.usecase.cnh.view.directmessage.DirectMessageHandler@1911 |

| | | |
|---|---|---|
| 25 | 0:21 | proftpd: (accepting connections) |
| 59 | 24:36 | /usr/bin/java -Djava.util.logging.config.file=/home/fcatomcat/tomcat8/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Xms4096m -Xmx12288m -XX:NewSize=4096m -XX:MaxNewSize=12288m -XX:PermSize=4096m -XX:MaxPermSize=12288m -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Djava.library.path=/usr/lib/x86_64-linux-gnu -classpath /home/fcatomcat/tomcat8/bin/bootstrap.jar:/home/fcatomcat/tomcat8/bin/tomcat-juli.jar -Dcatalina.base=/home/fcatomcat/tomcat8 -Dcatalina.home=/home/fcatomcat/tomcat8 -Djava.io.tmpdir=/home/fcatomcat/tomcat8/temp org.apache.catalina.startup.Bootstrap start |
| 22 | 0:00 | _ /bin/sh -c ps wauxf |

## Sessions

| Session id | Last access | Age | Expiration | Number of attributes | S |
|---|---|---|---|---|---|
| [redacted] | 00:00:00 | 01:44:51 | 4/29/21 4:23 PM | 5 | |
| [redacted] | 00:00:05 | 03:19:12 | 4/29/21 4:22 PM | 19 | |
| [redacted] | 00:00:08 | 00:48:36 | 4/29/21 4:22 PM | 5 | |
| [redacted] | 00:00:18 | 00:36:00 | 4/29/21 4:22 PM | 18 | |
| [redacted] | 00:00:25 | 03:20:25 | 4/29/21 4:22 PM | 5 | |
| [redacted] | 00:00:43 | 01:51:47 | 4/29/21 4:22 PM | 16 | |
| [redacted] | 00:00:52 | 00:17:08 | 4/29/21 4:22 PM | 18 | |
| [redacted] | 00:01:01 | 01:16:31 | 4/29/21 4:22 PM | 18 | |
| [redacted] | 00:01:14 | 03:21:06 | 4/29/21 4:21 PM | 5 | |
| [redacted] | 00:01:32 | 01:31:41 | 4/29/21 4:21 PM | 18 | |
| [redacted] | 00:01:46 | 01:42:38 | 4/29/21 4:21 PM | 18 | |
| [redacted] | 00:02:14 | 01:45:48 | 4/29/21 4:20 PM | 22 | |
| [redacted] | 00:02:25 | 00:17:29 | 4/29/21 4:20 PM | 16 | |
| [redacted] | 00:03:02 | 03:13:26 | 4/29/21 4:20 PM | 18 | |
| [redacted] | 00:03:17 | 00:48:36 | 4/29/21 4:19 PM | 21 | |
| [redacted] | 00:03:22 | 03:19:58 | 4/29/21 4:19 PM | 18 | |
| [redacted] | 00:03:27 | 01:51:54 | 4/29/21 4:19 PM | 5 | |
| [redacted] | 00:03:36 | 01:48:22 | 4/29/21 4:19 PM | 16 | |
| [redacted] | 00:03:37 | 01:49:36 | 4/29/21 4:19 PM | 6 | |
| [redacted] | 00:04:08 | 03:19:50 | 4/29/21 4:18 PM | 17 | |
| [redacted] | 00:04:17 | 03:19:17 | 4/29/21 4:18 PM | 5 | |

## Details session [redacted]

| Session id | Last access | Age | Expiration | Number of attributes | Serializable | |
|---|---|---|---|---|---|---|
| [redacted] | 00:01:43 | 05:03:01 | 4/28/21 10:41 PM | 20 | no | |

### Attributes

| Name | Type | Serializable | Serializable size (b) | |
|---|---|---|---|---|
| topMenuButton_0 | java.lang.String | yes | 11 | null |
| _____uc_DOMAIN_ID | java.lang.Long | yes | 82 | 1 |
| GDSP_STEP_PREFIX_baseReportTasks | java.lang.Integer | yes | 81 | 6 |
| ScopeMenuHandler | br.com.usecase.cnh.view.menu.scope.ScopeMenuHandler | no | -1 | br.com.usecase.cnh.view.menu.scope.ScopeMenuHandler@[redacted] |
| javamelody.userAgent | java.lang.String | yes | 121 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.9 |
| GDSP_STEP_PREFIX_dealershipSelectorQPV | java.lang.Integer | yes | 81 | 1 |
| javamelody.remoteAddr | java.lang.String | yes | 2[redacted] | |
| javamelody.country | java.lang.String | yes | 9 | BR |
| topMenuButton_3 | java.lang.String | yes | 11 | null |
| GDSP_TOTAL_PREFIX_baseReportTasks | java.lang.Integer | yes | 81 | 4 |
| topMenuButton_2 | java.lang.String | yes | 11 | null |
| DirectMessageHandler-Object | br.com.usecase.cnh.view.directmessage.DirectMessageHandler | no | -1 | br.com.usecase.cnh.view.directmessage.DirectMessageHandler@4dc7e08b |
| ___uc_AUTHENTICATED_USER | br.com.usecase.fwcnh.common.security.AuthenticatedUser | yes | 629 | AuthenticatedUser [id=[redacted] name=[redacted] |
| topMenuButton_1 | java.lang.String | yes | 11 | null |
| javamelody.sessionActivation | net.bull.javamelody.SessionListener | yes | 75 | SessionListener[sessionCount=15] |
| | | | | <li class=" minutes minutesList minutes report minutesGeneralReport actionPlan actionPlanList acti |

| Error |
| --- |
| WARN [org.hibernate.hql.internal.ast.QueryTranslatorImpl] HHH000104: firstResult/maxResults specified with collection fetch; applying in memory! |

## Current requests

None

## System information

Execute the garbage collector | Generate a heap dump | View memory histogram | Invalidate http sessions | View http sessions
View deployment descriptor | MBeans | View OS processes | JNDI tree

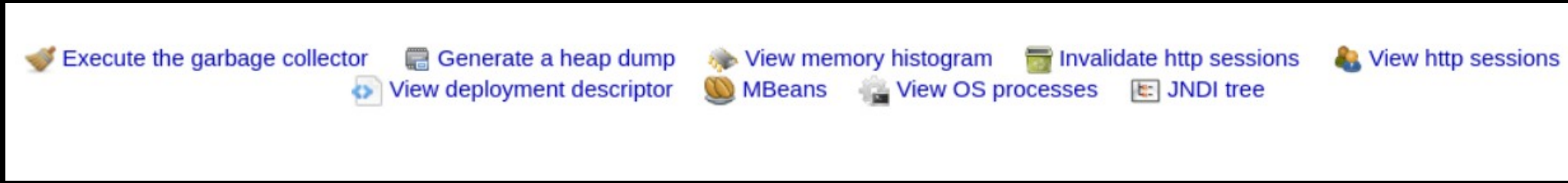
| | |
| --- | --- |
| Host: | [redacted] |
| Java memory used: | 1,099 Mb / 8,192 Mb |
| Nb of http sessions: | 9 |
| Nb of active threads (current http requests): | 0 |
| Nb of active jdbc connections: | 0 |
| Nb of used jdbc connections (opened if no datasource): | 0 |
| System load | 0.67 |
| % System CPU | 1.48 |

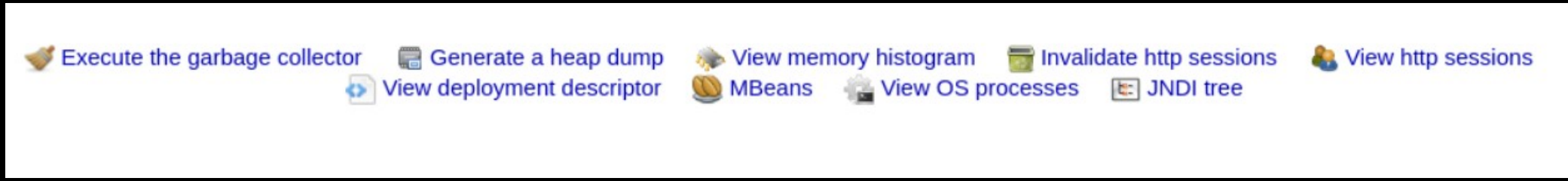
Details

## Threads

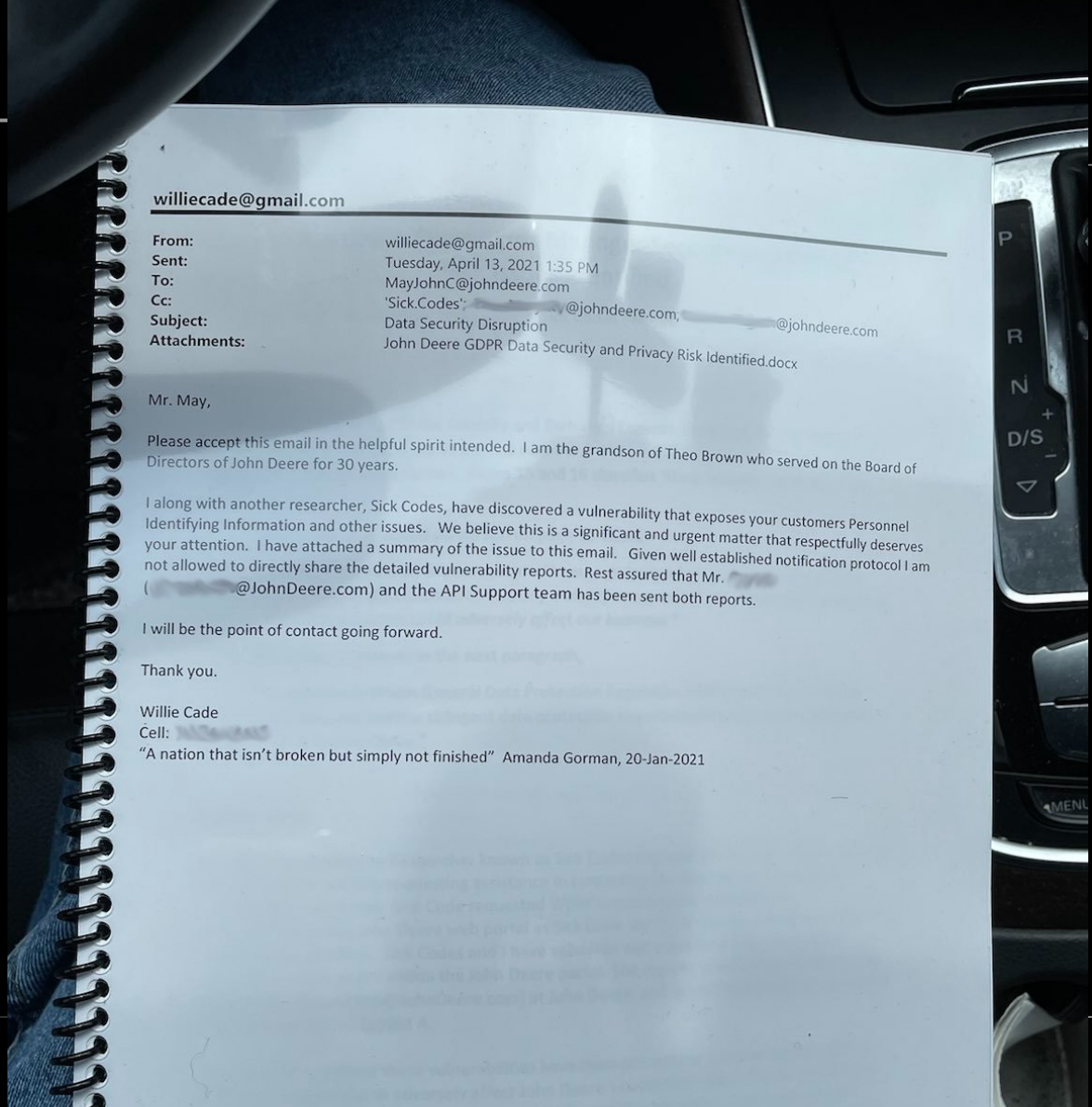
**Threads on** [redacted] Number = 54, Maximum = 54, Total started = 679 Details

Last collect time: 68 ms
Display time: 06 ms


Execute the garbage collector
Generate a heap dump
View memory histogram
Invalidate http sessions
View http sessions
View deployment descriptor
MBeans
View OS processes
JNDI tree


Execute the garbage collector
Generate a heap dump
View memory histogram
Invalidate http sessions
View http sessions
View deployment descriptor
MBeans
View OS processes
JNDI tree


Invalidate http sessions



williecade@gmail.com

**From:** williecade@gmail.com
**Sent:** Tuesday, April 13, 2021 1:35 PM
**To:** MayJohnC@johndeere.com
**Cc:** 'Sick.Codes'; [redacted]@johndeere.com; [redacted]@johndeere.com
**Subject:** Data Security Disruption
**Attachments:** John Deere GDPR Data Security and Privacy Risk Identified.docx

Mr. May,

Please accept this email in the helpful spirit intended. I am the grandson of Theo Brown who served on the Board of Directors of John Deere for 30 years.

I along with another researcher, Sick Codes, have discovered a vulnerability that exposes your customers Personnel Identifying Information and other issues. We believe this is a significant and urgent matter that respectfully deserves your attention. I have attached a summary of the issue to this email. Given well established notification protocol I am not allowed to directly share the detailed vulnerability reports. Rest assured that Mr. [redacted] ([redacted]@JohnDeere.com) and the API Support team has been sent both reports.

I will be the point of contact going forward.

Thank you.

Willie Cade
Cell: [redacted]
"A nation that isn't broken but simply not finished" Amanda Gorman, 20-Jan-2021

# COMPLIANCE

CNH Industrial believes that operating in a socially responsible and ethical manner and in compliance with the laws of those countries in which we operate is fundamental to our long-term success. This means, among other things, that we adopt fair employment practices, protect safety in the workplace, support and foster environmental consciousness and fully comply with applicable laws.

**CNH Industrial Compliance Helpline**

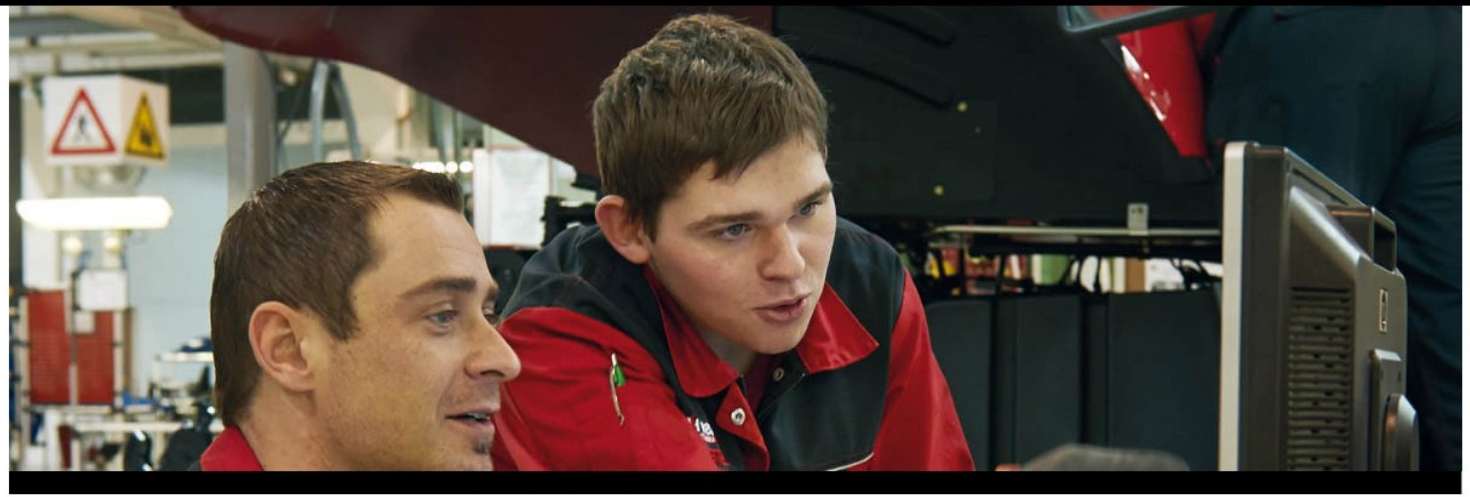
The Board of Directors has established a procedure to ensure that the Company's employees and third parties have the possibility to report alleged irregularities of a general, operational and financial nature with the Company.

The Company's compliance helpline is managed by an independent third party and is available 24 hours per day/seven days per week/365 days per year. Reports may be submitted through a dedicated web portal (www.cnhindustrialcompliancehelpline.com), by phone (to a call center managed by a third party), or to a Company representative. Where legally permissible, reports may be submitted on an anonymous basis. In addition, where legally required, the nature of the reports may be limited to certain subject matters. The Company investigates reports submitted and, in appropriate cases, implements corrective actions.

If you become aware of a circumstance or action that violates, or appears to violate, CNH Industrial's Code of Conduct, company policies or applicable law, you can seek guidance, or report a violation, by using the CNH Industrial Compliance Helpline, available at www.cnhindustrialcompliancehelpline.com.

## Related Links

HEALTH AND SAFETY POLICY



# Our Compliance Helpline

This tool is available to all our stakeholders, such as employees, customers, dealers and suppliers, for asking a question or reporting possible violations of our Code of Conduct, other policies or applicable laws. You may choose to submit a report by providing contact information, which will be held in the strictest of confidence.

Read More...

?

**ASK A QUESTION**

Click here if you have a question about our Code of Conduct

!

**RAISE A CONCERN**

Click here to raise a concern about unethical behavior in the workplace

**FOLLOW UP**

Click here to follow up on a previously submitted question or concern


632 8 comments

Like Comment Share Send

Reactions

Comments Most relevant

**Sick Codes** 1w
Security Researcher, Freelance Automation Speci...

Can someone at CNH get in touch regarding a possible security vulnerability?

Like Reply • 1 reply

**Sick Codes** 5d
Security Researcher, Freelance Automation...

Still waiting, multiple phone calls and emails, please get in touch.

Like Reply

Leave your thoughts here... @ Post

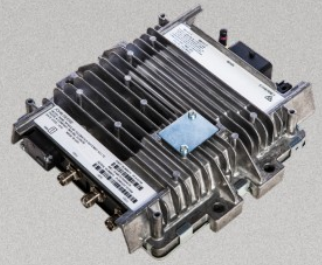
Home My Network Post Notifications 1 Jobs


CNH
INDUSTRIAL
SHIPPING & RECEIVING
Use phone @ gate for access
SECURITY OFFICE
HUMAN RESOURCES

# MTG 4G LTE

The Modular Telematics Gateway integrates GNSS, mobile connectivity and on-board machine communications via CAN, Ethernet, and RS-232. It's ideally suited for advanced telematics applications such as machine health monitoring, advanced logistics, and remote diagnostics.

The Modular Telematics Gateway integrates GNSS, mobile connectivity and on-board machine communications via CAN, Ethernet, and RS-232. It's ideally suited for advanced telematics applications such as machine health monitoring, advanced logistics, and remote diagnostics.



Storage: 8GB onboard flash

Designed and tested to extreme environments

Supports LTE with fallback to 3G and 2G cellular communication

Supports 12V and 24V systems

Open source created with Yocto Project® software*

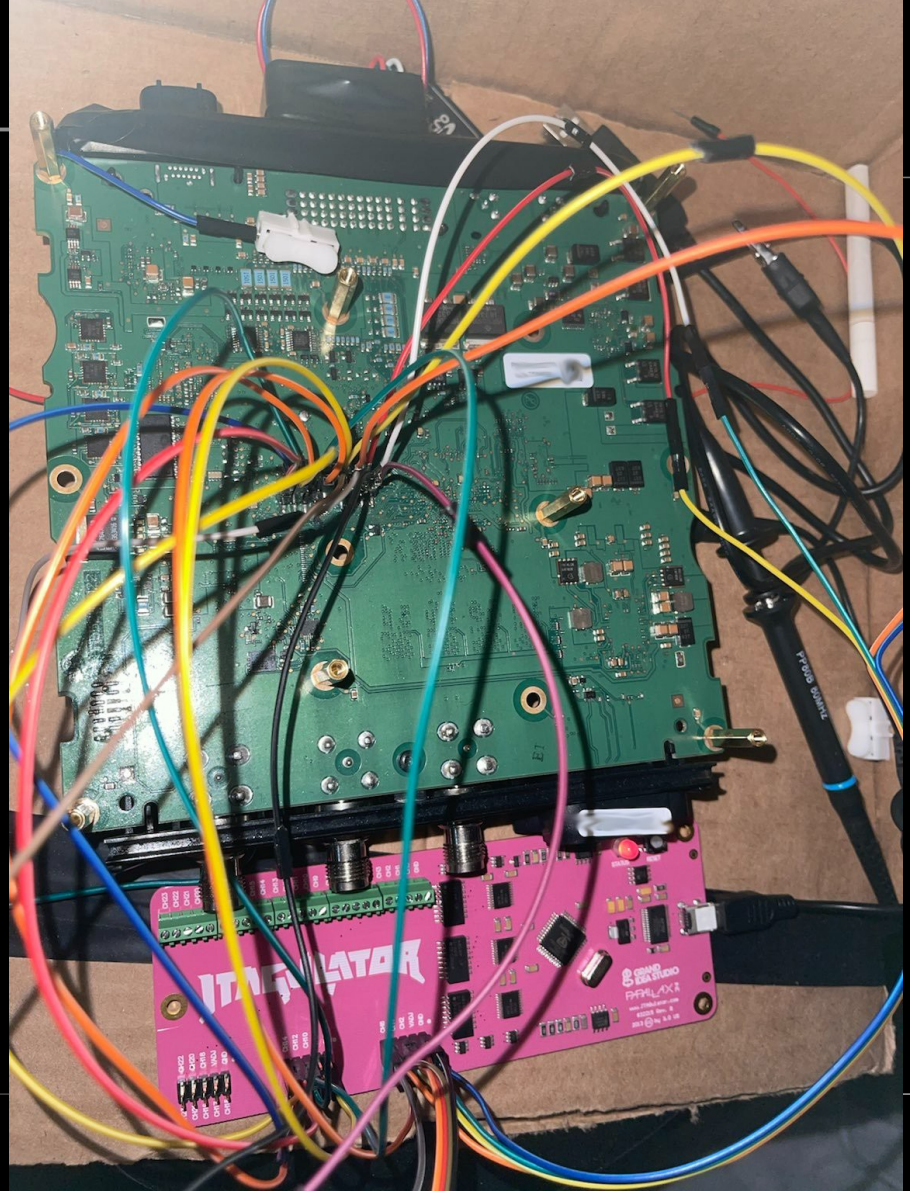
Supports multiple SIM options:
- Internal soldered SIM IC
- External accessible Micro-SIM
- Combination of internal and external SIM

Wireless and Bluetooth® communication

Certified in over 70 countries

*Linux® and Yocto Project® are registered trademarks of the Linux Foundation. Linux® is a registered trademark of Linux Benedict Torvalds.


JOHN DEERE
MODEL NAME: MODULAR TELEMATICS GATEWAY 4G LTE
DEERE & COMPANY - MOLINE, IL 61265
MADE IN USA
CELL
GPS
CELL
MAIN
ETHERNET


PARLAX

## Third Party Software Notifications and Licenses

The copyrights for certain portions of the Software may be owned or licensed by other third parties ("Third Party Software") and used and distributed under license. The Third Party Notices include the acknowledgements, notices, and licenses for the Third Party Software. The Third Party Notices are available on the CD included with this Operator's Manual. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in the applicable Software End User License Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licences.

Copies of those licenses are included in the Third Party Notices.

You may obtain the complete Corresponding Source Code from us for a period of three years after our last shipment of the Software by sending a request letter to:

Deere Open Source Compliance Team
P.O. Box 1202
Moline, IL 61266-1202 USA

Please include "source for John Deere MTG 4G LTE" and the version number of the software in the request letter. This offer is valid to anyone in receipt of this information.

AE77568,000020D -19-23JUN16-1/1

- https://www.qualcomm.com/company/product-security/bulletins

| Public ID | Security Rating | CVSS Rating | Technology Area | Date Reported |
|---|---|---|---|---|
| CVE-2020-11307 | Critical | Critical | Data Network Stack & Connectivity | Internal |
| CVE-2021-1886 | Critical | High | HLOS | Internal |
| CVE-2021-1888 | Critical | High | HLOS | Internal |
| CVE-2021-1889 | Critical | High | HLOS | Internal |
| CVE-2021-1890 | Critical | High | HLOS | Internal |
| CVE-2021-1887 | High | High | WLAN Firmware | 08/06/2020 |
| CVE-2021-1938 | High | High | WLAN Firmware | 11/20/2020 |
| CVE-2021-1953 | High | High | WLAN Firmware | 12/16/2020 |

This table lists moderate security vulnerabilities. OEMs have been notified and encouraged to patch these issues.

# Thank you.

- Sick Codes https://twitter.com/sickcodes
- wabaf3t https://twitter.com/wabafet1
- D0rkerDevil https://twitter.com/D0rkerDevil
- johnjhacking https://twitter.com/johnjhacking
- rej_ex https://twitter.com/rej_ex
- w0rmer https://twitter.com/0x686967
- ChiefCoolArrow https://twitter.com/ChiefCoolArrow
- Kelly https://twitter.com/kaoudis
- Willie Cade https://twitter.com/WillieCade7
- Kevin Kenney https://twitter.com/GrassrootsKK