16 [redacted] exposes sensitive shipment information to public web

Share:

State	Resolved (Closed)
Disclosed	April 8, 2019 9:31pm +0530
Reported To	U.S. Dept Of Defense
Weakness	Information Disclosure
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

cablej_dds submitted a report to U.S. Dept Of Defense. Aug 1st (about 1 year ago)

Summary:

A subdomain of the [redacted] site exposes sensitive shipment information to the public web at [redacted]downloads/xfer_fak. Although I haven't been able to find too much info about this, it seems to be fairly sensitive and updated daily, containing over 500,000 lines just for 07/30/18. Information included looks to be many/all shipments routed under [redacted]:

```
The [redacted] system IS an
automated U S [redacted] Command ([redacted]) and U S [redacted]
Military [redacted] [redacted] Command ([redacted]) [redacted] management
web-based system [redacted] IS the single manager of DoD [redacted]
[redacted] and IS responsible for acceptance and approval of[redacted] of
service from the U S [redacted] [redacted] has developed the [redacted]
system as an automated web-based [redacted] [redacted] management
system With an integrated [redacted] [redacted] database [redacted] provides an automated
electronic commerce capability for the procurement of [redacted]
[redacted] services as well as a real time data feed to war fighters
```

[redacted]]

Information exposed includes route information, contact names / phone numbers for each shipment,
shipment cost, content information, hazmat risk, classification level (U or C or S, likely unclass / confidential / secret), and more.

Some interesting ones:

The first listed indicates[redacted] materials and originates from the [[redacted]]([redacted]), which is used to maintain [redacted]....

```
0               DOMESTIC FREIGHT ROUTING REQUEST AND ORDER
================================================================================
Requestor..: [redacted]                        Ship ID..: [redacted]
Phone / FAX: [redacted]/                   From.....: 0
Agency ID..:              Ship.Type: B        Miles: 1676  Total Miles: 1745

Origin: [redacted]       ;[redacted]             Destin: [redacted]       ;[redacted]

[redacted] [redacted]     , ND SPLC: [redacted]       [redacted] [redacted]    , GA SPLC: [redacted]
 Rail Siding: N     SCAC:               Rail Siding: N     SCAC:
----- Nearest Rail Point -----------    ----- Nearest Rail Point -----------


SCAC Requested/Received: 999/7          Conveyances: 1         Urgent: N
```

```
██ Priority: 2              Sec. Risk..: C C C C C C C C C C *
Availability Date......: 08/01/18       HazMat.....: H████████ ████
Desired Delivery Date..: 08/03/18       Over Dimen.: n/a
Shipment Total WT/VOL..:    10187.00 Pds Disability.: None
Shipment Cube (CuFt)...:         489.00  Line Items.: 34
Movement Modes.........: B              Services...: ███████
Export.................: N              Type of RO.: D    Mil Svc Code: F


 Ship ID: ████████   CONVEYANCE DETAIL
 ------------------------------------------------------------------------------
 Conv:  1              Mode [B] Other      Cube-Ft:    489  TotWt/Vol:   10187
 Ordered Veh(s) [  1]   Cap Load   [N]      P/G/B:  P        Overweight:     N
 Overdimensional: N Length:    0 Width:    0 Height:      0  Pallet Wt :
 Equipment        [AV3]   [   ]   [   ]   [   ]   [   ]   [   ]   [   ]   [   ]

 1. Commodity   [  062820] Radio, Radio-telephone or Televis
    FAK         [  999912] Vehicles Moved:    Security Risk:   Y

 2. Commodity   [16490001] Radioactive Materials, Articles Or    H█████       ██
    FAK         [        ] Vehicles Moved:    Security Risk:   Y

 3. Commodity   [  061700] Electrical Appliances or Instrume
    FAK         [  999912] Vehicles Moved:    Security Risk:   Y

 4. Commodity   [  060535] Aerials or Antennas, or Parts the
    FAK         [  999912] Vehicles Moved:    Security Risk:   Y

 5. Commodity   [        ]
    FAK         [        ] Vehicles Moved:    Security Risk:
 ------------------------------------------------------------------------------
```

```
0               DOMESTIC FREIGHT ROUTING REQUEST AND ORDER
================================================================================
Requestor..: ███████                      Ship ID..: ████████
Phone / FAX: ██████/                   From.....: 0
Agency ID..:              Ship.Type: B        Miles: 2289  Total Miles: 2289

Origin: ███████       ;███████             Destin: █████████       ;██████

█████████ , ██ SPLC: ████       ███ ████     , ████████: ██████████
 Rail Siding: N     SCAC:                Rail Siding: N     SCAC:
----- Nearest Rail Point -----------    ----- Nearest Rail Point -----------


SCAC Requested/Received: 45/1           Conveyances: 1          Urgent: N
████████ Priority: 2              Sec. Risk..: S
Availability Date......: 07/30/18       HazMat.....: None
Desired Delivery Date..: 07/31/18       Over Dimen.: n/a
Shipment Total WT/VOL..:        1.00 Pds Disability.: None
Shipment Cube (CuFt)...:           1.00  Line Items.: 1
Movement Modes.........: K              Services...: CIS
Export.................: Y              Type of RO.: D    Mil Svc Code: F


 Ship ID: ████   CONVEYANCE DETAIL
 ------------------------------------------------------------------------------
 Conv:  1              Mode [K] Other      Cube-Ft:      1  TotWt/Vol:       1
 Ordered Veh(s) [  1]   Cap Load   [N]      P/G/B:  P        Overweight:     N
 Overdimensional: N Length:    0 Width:    0 Height:      0  Pallet Wt :
 Equipment        [QQ ]   [   ]   [   ]   [   ]   [   ]   [   ]   [   ]   [   ]
```

```
1. Commodity   [  063470] Tubes, vacuum, electronic or radi
   FAK         [  999912] Vehicles Moved:    Security Risk:   Y

2. Commodity   [        ]
   FAK         [        ] Vehicles Moved:    Security Risk:

3. Commodity   [        ]
   FAK         [        ] Vehicles Moved:    Security Risk:

4. Commodity   [        ]
   FAK         [        ] Vehicles Moved:    Security Risk:

5. Commodity   [        ]
   FAK         [        ] Vehicles Moved:    Security Risk:
--------------------------------------------------------------------------------
```

```
LINE ITEM DETAIL
--------------------------------------------------------------------------------
NO  PK/VCL TYPE   NEW      COMMODITY LEN  WID  HGT  CUBE    QUANTITY  FCC STOP
      DESCRIPTION
--------------------------------------------------------------------------------

1.      1 CTN             999913     16   10   10      1        4-P

      UN-ID.................: ███████
      PROPER SHIPPING NAME..: CARTRIDGES, POWER DEVICE
      UN CLASS..............:  1.4C
      FLASH POINT...........:
      NET EXPLOSIVE QUANTITY: 1 LB
      REPORTABLE QUANTITY...:
      PACKING GROUP.........:
      TOTAL QUANTITY........: 0 LB

2.      1 CTN             999913     10   10   16      1        3-P

      UN-ID.................: ██████
      PROPER SHIPPING NAME..: CARTRIDGES, POWER DEVICE
      UN CLASS..............:  1.4C
      FLASH POINT...........:
      NET EXPLOSIVE QUANTITY: 1 LB
      REPORTABLE QUANTITY...:
      PACKING GROUP.........:
      TOTAL QUANTITY........: 0 LB
```

Step-by-step Reproduction Instructions

1. Visit ████/████downloads/xfer_fak.
2. Wait for the 30 mb response to download.
3. Observe that this lists over 500,000 lines of a daily summary of shipments. See above for several examples.

Impact

Not sure of the full contextual impact, but it's safe to say that this info should definitely not be publicly accessible. Day-to-day logs of over 500k lines with details of every shipment.

cablej_dds posted a comment. Aug 1st (about 1 year ago)

Confirmed that this is updated daily. There's now completely new info for 07/31/18.

ag3nt-j1 updated the severity to High. Aug 1st (about 1 year ago)

ag3nt-j1 changed the status to ○ **Triaged**. Aug 1st (about 1 year ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-j1 closed the report and changed the status to ○ **Resolved**. Aug 15th (about 1 year ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

cablej_dds requested to disclose this report. Apr 4th (6 months ago)

Hi,

As mentioned in the email, I would like to disclose this report in order to demo at an upcoming event.

Thank you,
Jack

ag3nt-j1 agreed to disclose this report. Apr 8th (6 months ago)

This report has been disclosed. Apr 8th (6 months ago)