



eCSIRT.net The European CSIRT Network

**Status Update
TF-CSIRT, September 2003
Amsterdam, NL**

© 2000-2003 by PRESECURE® Consulting GmbH



Review of the current results

- **Statistics – Clearinghouse function**
- **Infrastructure – Alert function**

Slide 2

© 2000-2003 by PRESECURE® Consulting GmbH



Participation

■ Participation is restricted to teams that are:

- Partners of the eCSIRT.net project
- Liaisons of the eCSIRT.net project
 - Any TI accredited team by default
 - Any other team by decision of the project partners

■ furthermore

- The Code-of-Conduct must be signed
- The related Policies must be accepted

Slide 3

© 2000-2003 by PRESECURE® Consulting GmbH



Type 1 Statistics

■ (Meta) Information on the **Workload**

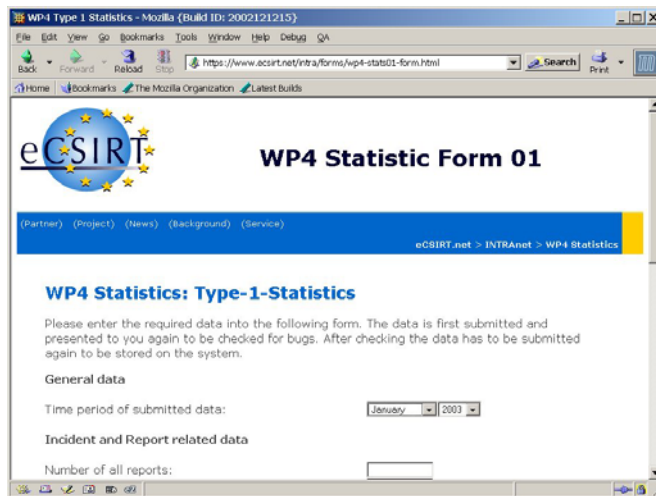
- Either a product of human assessment or
- derived from tracking data by IH tools
- Characteristic data points:
 - reports and incidents / attacks
 - affected systems, persons, organizations
 - time spent
- Reporting ensures authenticity and confidentiality
- Access of participating CSIRTs to aggregated data
- Subset of aggregated data as public available statistics

Slide 4

© 2000-2003 by PRESECURE® Consulting GmbH



Type 1 Statistics Form



The screenshot shows a Mozilla browser window with the address bar displaying `https://www.ecsirt.net/intra/forms/wp4-stat01-form.html`. The page title is "WP4 Type 1 Statistics - Mozilla (Build ID: 2002121215)". The page content includes the eCSIRT logo, the title "WP4 Statistic Form 01", and a navigation bar with links: (Partner) (Project) (News) (Background) (Service). Below the navigation bar, the page is titled "WP4 Statistics: Type-1-Statistics". A paragraph explains the data submission process: "Please enter the required data into the following form. The data is first submitted and presented to you again to be checked for bugs. After checking the data has to be submitted again to be stored on the system." The form is divided into two sections: "General data" and "Incident and Report related data". The "General data" section contains a "Time period of submitted data:" label with a dropdown menu showing "January" and "2003". The "Incident and Report related data" section contains a "Number of all reports:" label with an empty text input field.

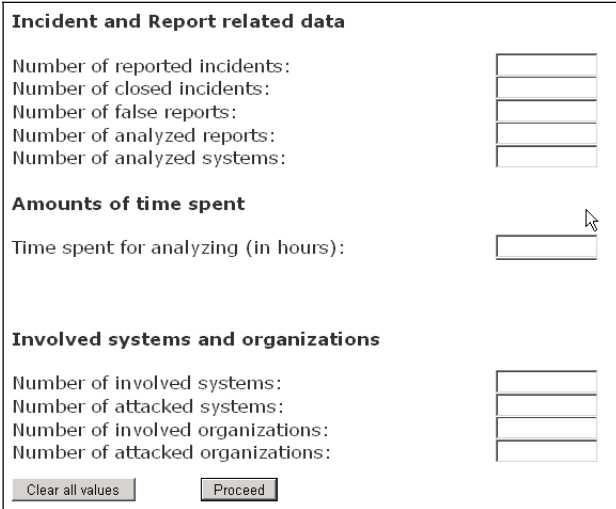
- Monthly reporting
- Web form
- SSL Client Certificates

Slide 5

© 2000-2003 by PRESECURE® Consulting GmbH



Type 1 Statistics Form (2)



The screenshot shows the "Incident and Report related data" section of the form. It contains five labels with corresponding text input fields: "Number of reported incidents:", "Number of closed incidents:", "Number of false reports:", "Number of analyzed reports:", and "Number of analyzed systems:". Below these is the "Amounts of time spent" section, which includes a label "Time spent for analyzing (in hours):" and a text input field. The "Involved systems and organizations" section follows, with four labels and text input fields: "Number of involved systems:", "Number of attacked systems:", "Number of involved organizations:", and "Number of attacked organizations:". At the bottom of the form are two buttons: "Clear all values" and "Proceed".

Slide 6

© 2000-2003 by PRESECURE® Consulting GmbH



Type 2 Statistics

- Information on **Incidents** handled by CERTs:
 - Information submitting monthly by CERTs for closed incidents
 - Information submitted is based on IODEF classification scheme
 - Reporting ensures authenticity and confidentiality
 - Access of participating CSIRTs to aggregated data
 - Subset of aggregated data as public available statistics



Slide 7

© 2000-2003 by PRESECURE® Consulting GmbH

Type 2 Statistics Form

A screenshot of a web browser window titled "WP4 Type 2 Statistics - Mozilla (Build ID: 2002121215)". The address bar shows the URL "https://www.ecsirt.net/intra/forms/wp4-stats02-form.html". The page content includes a paragraph of text, a "General Data" section with a date selector, and a "Policy Violations" section with a table for incident types.

Many thanks to Jimmy Arvidsson, Tella CERTCC. This classification scheme is based on his Incident Taxonomy.

In each row enter the number of Incidents of the according type. Each Incidents has ONE primary type (so the numbers given for primary type add up to the number of all Incidents). Incidents can belong to additional types. The number of Incidents whose secondary types are of the requested type should be entered in the secondary type column. These numbers do not have to add up to the total number of Incidents.

General Data

Time period of submitted data:

Policy Violations

	primary type (mandatory)	additional types (optional)
Violation of Acceptable Use Policy:	<input type="text"/>	<input type="text"/>
Violation of Corporate Policy:	<input type="text"/>	<input type="text"/>
Violation of National Laws:	<input type="text"/>	<input type="text"/>
Hoaxes:	<input type="text"/>	<input type="text"/>
Harassment:	<input type="text"/>	<input type="text"/>

Slide 8

© 2000-2003 by PRESECURE® Consulting GmbH



Type 2 Statistics Form (2)

Malicious Code

Virus:	<input type="text"/>	<input type="text"/>
Worm:	<input type="text"/>	<input type="text"/>
Trojan:	<input type="text"/>	<input type="text"/>
Spyware:	<input type="text"/>	<input type="text"/>
Dialer:	<input type="text"/>	<input type="text"/>

Information Gathering

Scanning:	<input type="text"/>	<input type="text"/>
Probing:	<input type="text"/>	<input type="text"/>
Sniffing:	<input type="text"/>	<input type="text"/>
Social Engineering:	<input type="text"/>	<input type="text"/>

Intrusion Attempts

Exploiting of known Vulnerabilities:	<input type="text"/>	<input type="text"/>
Login attempts:	<input type="text"/>	<input type="text"/>
New attack signature:	<input type="text"/>	<input type="text"/>

Slide 9

© 2000-2003 by PRESECURE® Consulting GmbH



Type 2 Statistics Form (3)

Intrusions

Privileged Account Compromise:	<input type="text"/>	<input type="text"/>
Unprivileged Account Compromise:	<input type="text"/>	<input type="text"/>
Application Compromise:	<input type="text"/>	<input type="text"/>

Availability

DoS:	<input type="text"/>	<input type="text"/>
DDoS:	<input type="text"/>	<input type="text"/>
Sabotage:	<input type="text"/>	<input type="text"/>

Information Security

Unauthorised access to information:	<input type="text"/>	<input type="text"/>
Unauthorised modification of information:	<input type="text"/>	<input type="text"/>

Fraud

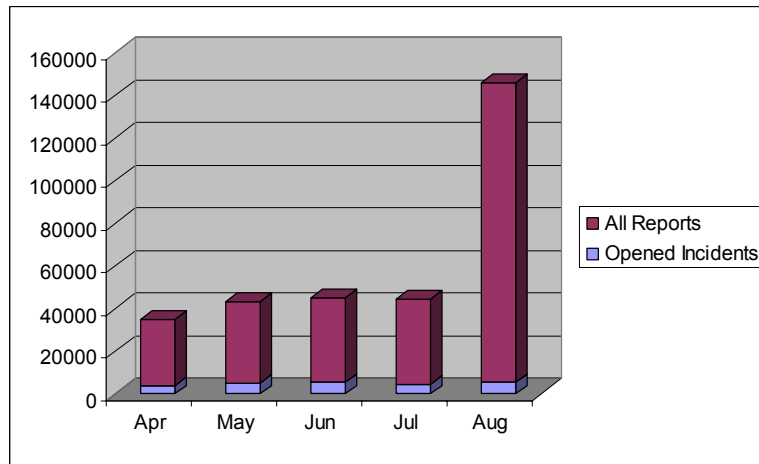
Unauthorized use of resources:	<input type="text"/>	<input type="text"/>
Copyright:	<input type="text"/>	<input type="text"/>
Masquerade:	<input type="text"/>	<input type="text"/>

Slide 10

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 1 (5 Teams)

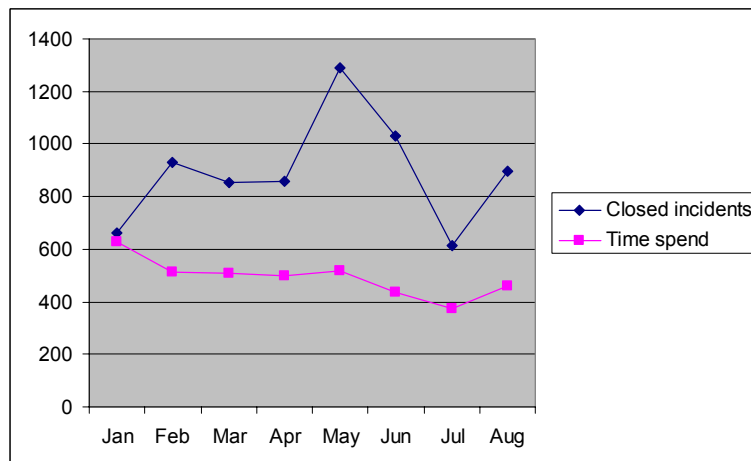


Slide 11

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 1 (3 Teams)

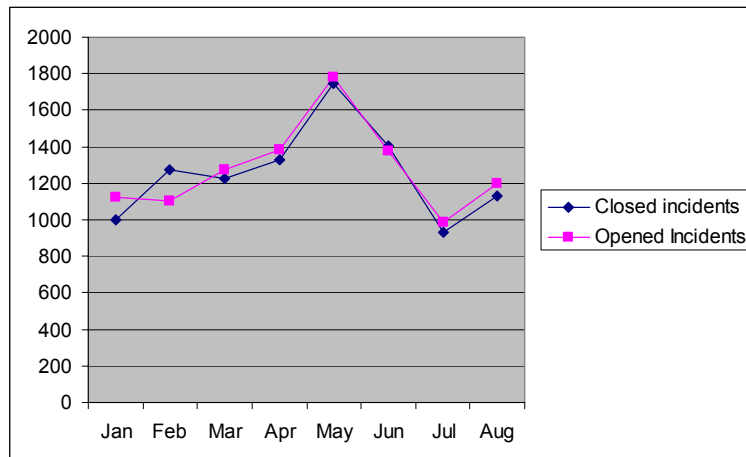


Slide 12

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 1 (4 Teams)

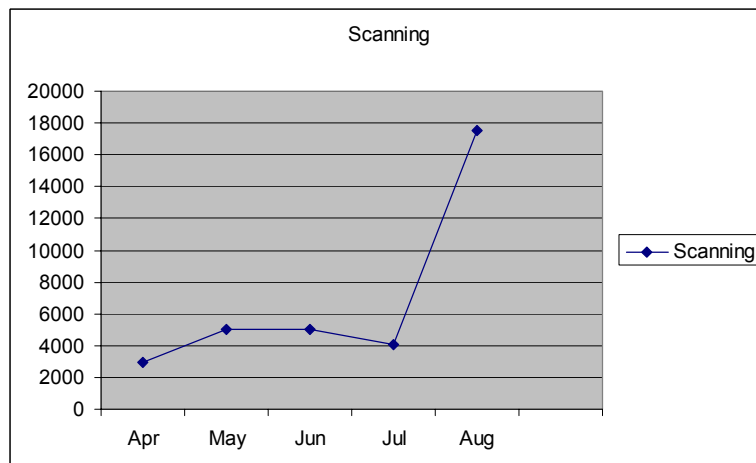


Slide 13

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 2 (3 Teams)

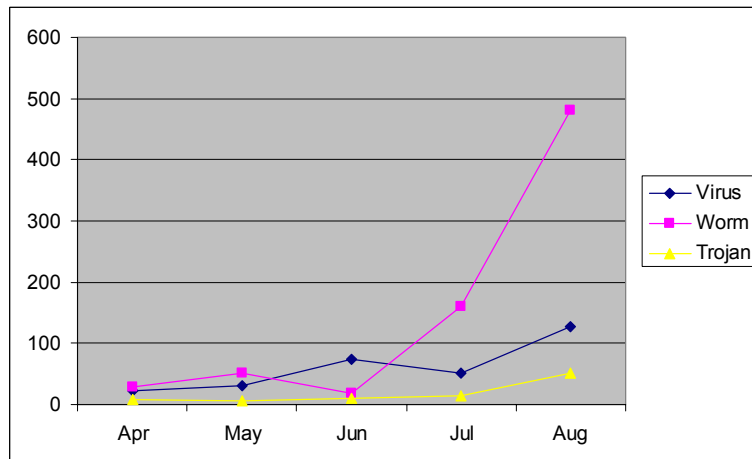


Slide 14

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 2 (3 Teams)

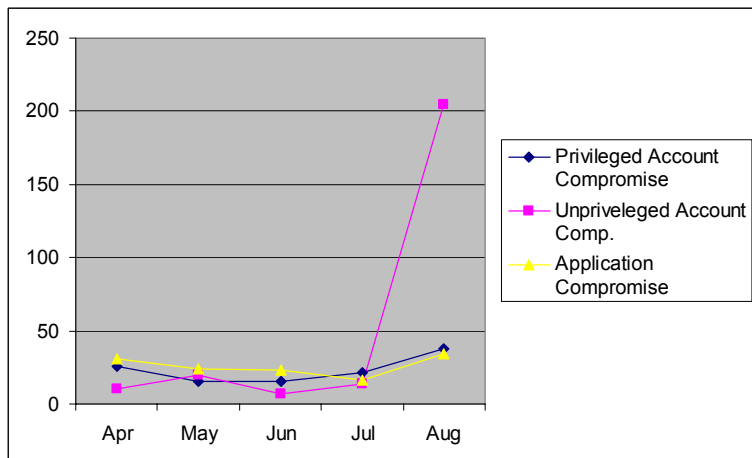


Slide 15

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 2 (3 Teams)

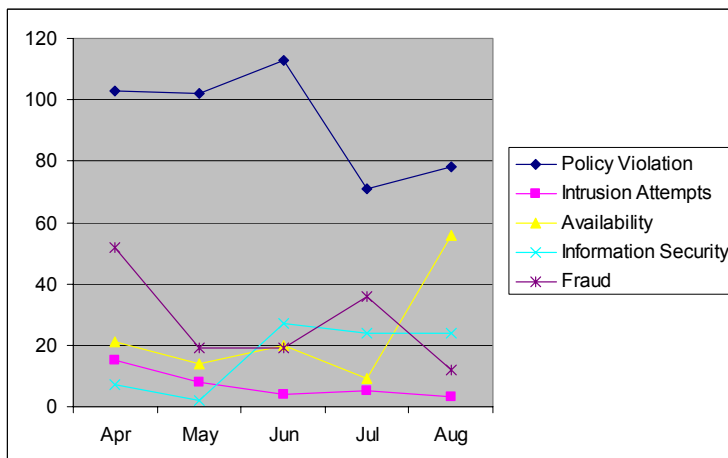


Slide 16

© 2000-2003 by PRESECURE® Consulting GmbH



Statistical Results: Type 2 (3 Teams)



Slide 17

© 2000-2003 by PRESECURE® Consulting GmbH



Type 3 Statistics

■ Information on **Events** on the Internet:

- Not necessarily handled by a CERT
- Not necessarily a successful intrusion
- Submission ensures authenticity (and confidentiality)
- Gathered and aggregated automatically
- Access of participating CSIRTs to aggregated data
- Subset of aggregated data as public available statistics

Slide 18

© 2000-2003 by PRESECURE® Consulting GmbH



Sensors for Type 3 Statistics

- **Sensor is located on not otherwise used system(s) reachable over the Internet**
 - HONEYD – to fake system (1 IP address)
 - Second IP address for reporting
- **Configuration of detection software**
 - Bootable CD-ROM image (GPL, free)
 - Configuration floppy (text based files)
 - Pregenerated public key pair for each sensor
- **Software**
 - PRELUDE – Network IDS with SNORT rule set
 - CRYPTO-NTP – to allow correlation
- **Exchange based on IDMEF**

Slide 19

© 2000-2003 by PRESECURE® Consulting GmbH



Centralized Collector for Type 3 Statistics

- **Services**
 - Crypto-NTP server
 - PRELUDE Collector
 - HTTPS protected web access to data
- **User Access via https and user certificates**
- **Manual key generation and management**
 - Sensor public key pairs
 - User und server certificates
 - CD-ROM image
 - Configuration files

Slide 20

© 2000-2003 by PRESECURE® Consulting GmbH



Type 3 Statistics Access

Alert List | HeartBeat | Top 15 Attackers | Top 15 Attacks | Statistics

Filter Factory | Edit current filter | DFN-CERT-Sensor | Load filter

Severity filter

☒ high
☒ medium
☒ low

Sort by

☒ timestamp
☐ group by key

Results per page

15

Delete

☒ nothing
☐ selected alerts
☐ alerts matched by filter

Group by

☐ Classification Name
☐ Source Address
☐ Target Port

Order

☒ Desc.
☐ Asc.

Since

1 day

Process

☒ nothing
☐ selected alerts
☐ alerts matched by filter

by program: None

submit

202 results for those filters

First Prev Last

P	Id	Classification	Impact	Type	Source	Destination	Sensor	Timestamp
906	906	HTTP escape sequence hide another sequence	other	tcp	146.145.25.67:1353 (relief)	193.174.13.136:80 (http)	NIDS	2003-08-28 14:58:27
905	905	HTTP escape sequence hide another sequence	other	tcp	146.145.25.67:1353 (relief)	193.174.13.136:80 (http)	NIDS	2003-08-28 14:58:27
904	904	WEB-IIS cmd.exe access	other	tcp	146.145.25.67:1340 (sbook)	193.174.13.136:80 (http)	NIDS	2003-08-28 14:58:27
903	903	WEB-IIS cmd.exe access	other	tcp	146.145.25.67:1347 (bbn-mmcc)	193.174.13.136:80 (http)	NIDS	2003-08-28 14:58:26
902	902	WEB-IIS CodeRed v2 root.exe access	other	tcp	146.145.25.67:1345 (vgip)	193.174.13.136:80 (http)	NIDS	2003-08-28 14:58:26
901	901	MS-SQL version overflow attempt	other	udp	213.77.250.225:1815 (mmpt)	193.174.13.136:1434 (ms-sql-m)	NIDS	2003-08-28 12:52:26

Slide 21

© 2000-2003 by PRESECURE® Consulting GmbH



Type 3 Statistics Access (2)

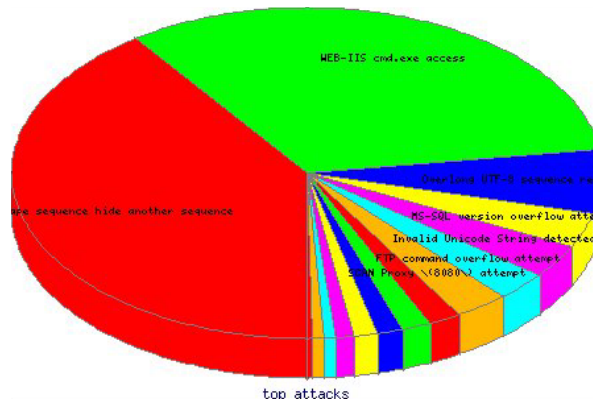
AttackNb	Attack name
250	HTTP escape sequence hide another sequence
202	WEB-IIS cmd.exe access
39	Overlong UTF-8 sequence received
21	MS-SQL version overflow attempt
20	Invalid Unicode String detected
18	FTP command overflow attempt
18	SCAN Proxy \ (8080\) attempt
11	ICMP PING NMAP
10	WEB-IIS ..\.. access
9	SCAN Squid Proxy attempt
8	WEB-IIS nsislog.dll access
6	ICMP PING CyberKit 2.2 Windows
4	ICMP supscan echo
4	WEB-IIS CodeRed v2 root.exe access
2	ICMP Destination Unreachable (Communication Administratively Prohibited)

Slide 22

© 2000-2003 by PRESECURE® Consulting GmbH



Type 3 Statistics Access (3)



Slide 23

© 2000-2003 by PRESECURE® Consulting GmbH



Attacking Hosts on multiple Sensors

```
$host> ./attackers_seen_per_sensor.pl -B
```

```
# 96240 attacks exist in database.
```

```
# alerts from 6 different sensors exist.
```

```
# alerts from 13332 different hosts exist.
```

```
13012 attacking hosts seen by 1 sensors.
```

```
242 attacking hosts seen by 2 sensors.
```

```
49 attacking hosts seen by 3 sensors.
```

```
23 attacking hosts seen by 4 sensors.
```

```
1 attacking hosts seen by 5 sensors.
```

```
5 attacking hosts seen by 6 sensors.
```

Slide 24

© 2000-2003 by PRESECURE® Consulting GmbH



Attack Methods per Host

```
$host> ./different_attacks_per_host.pl -B
```

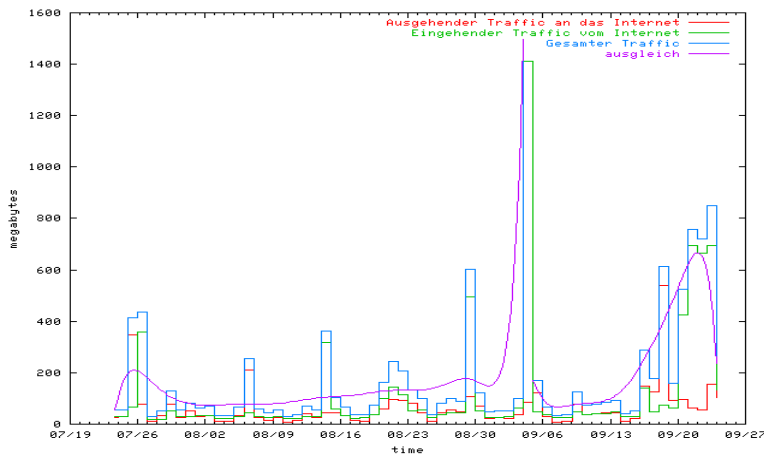
```
10075 hosts seen using 1 different attacks.  
1777 hosts seen using 2 different attacks.  
859 hosts seen using 3 different attacks.  
71 hosts seen using 4 different attacks.  
514 hosts seen using 5 different attacks.  
18 hosts seen using 6 different attacks.  
9 hosts seen using 7 different attacks.  
3 hosts seen using 9 different attacks.  
2 hosts seen using 10 different attacks.  
2 hosts seen using 11 different attacks.  
2 hosts seen using 14 different attacks.
```

Slide 25

© 2000-2003 by PRESECURE® Consulting GmbH



Our traffic has changed a little



Slide 26

© 2000-2003 by PRESECURE® Consulting GmbH



Alert Function - Status

■ Cryptographic secure mailing list

- Supports S/MIME and PGP
- Based on commercial SMTP proxy
- Secret key of mailing list for receiving emails
- Public keys of subscribers for sending emails

■ Status

- Operational

Slide 27

© 2000-2003 by PRESECURE® Consulting GmbH



Use of the Alert Function

■ Whenever there is a legitimate interest of the participating CSIRTs

■ If the impact can be foreseen and represents a widespread threat

- e.g. nationwide or international

■ Communication

- Native IODEF objects being send to the mailing list
- Web form to facilitate common format for alerts

Slide 28

© 2000-2003 by PRESECURE® Consulting GmbH



Alert Form

Alert Form - Mozilla (build ID: 2002121215)

File Edit View Go Bookmarks Tools Window Help Debug QA

Back Forward Reload Stop <https://www.ecsirt.net/infra/forms/wp5-alert-form.html> Search Print

Home Bookmarks The Mozilla Organization Latest Builds

WP5 Alert Function: version-1.0

Please enter the required data into the following form. The data is first submitted and presented to you again to be checked for bugs. After checking the data has to be submitted again to be distributed.

Incident

Restriction: ☒ eCSIRT.net ☐ need-to-know ☐ public

Incident ID:

Description:

Affected Platforms

Windows	Linux	Network	Other
95 98 ME NT	IBM AIX BSD Debian FreeBSD	3com Alcatel Allied Telesyn BinTec	Apple Mac OS FSC BS 2000 IBM OS390/400 HP OpenVMS

Systems:

Slide 29

© 2000-2003 by PRESECURE® Consulting GmbH



Alert Form (2)

Alert Form - Mozilla (build ID: 2002121215)

File Edit View Go Bookmarks Tools Window Help Debug QA

Back Forward Reload Stop <https://www.ecsirt.net/infra/forms/wp5-alert-form.html> Search Print

Home Bookmarks The Mozilla Organization Latest Builds

Software:

Server	Client	Other Software - Version
Apache DB2 Bind Kerberos	GPG Java KDE Konqueror	<input type="text"/>

Assessment

Type	Severity	Confidence
user root unknown	<input type="radio"/> high <input type="radio"/> medium <input type="radio"/> low	<input type="radio"/> high <input type="radio"/> medium <input type="radio"/> low

Method

Origin	Url
bugtraq cve certcc	<input type="text"/>

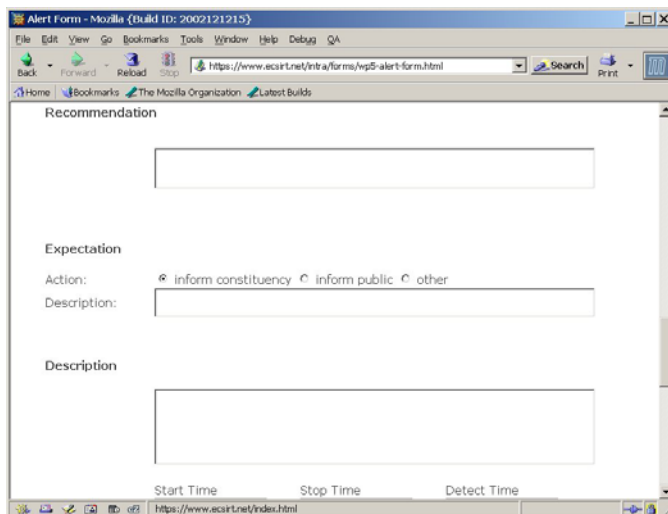
Description:

Slide 30

© 2000-2003 by PRESECURE® Consulting GmbH



Alert Form (3)



The screenshot shows a Mozilla browser window with the address bar displaying <https://www.ecsirt.net/nta/forms/wp5-alert-form.html>. The form is titled "Alert Form - Mozilla (build ID: 2002121215)". It contains several input fields and radio buttons. The "Recommendation" field is a large text area. The "Expectation" section has three radio buttons: "inform constituency" (selected), "inform public", and "other". The "Action:" field is a text input. The "Description:" field is a large text area. At the bottom, there are three checkboxes: "Start Time", "Stop Time", and "Detect Time". The status bar at the bottom shows the URL <https://www.ecsirt.net/index.html>.

Slide 31

© 2000-2003 by PRESECURE® Consulting GmbH



Alerts – Text format

Incident: PRE-CERT-0003
Date: 2003-08-28T10:56:00:00
Restriction: eCSIRT.net

Description: eCSIRT.net Test --- A buffer overrun vulnerability exists in the part of the Windows Remote Procedure Call (RPC) that deals with message exchange over TCP/IP (Port 135).

Affected systems: Windows: XP
NT, Windows 2000, Windows 2003 Server

Assessment: Severity: high
Type: admin
Confidence: high

Expectation: other: inform constituency

Method: Origin: vendor
Url: <http://www.microsoft.com/security/securitybulletins/ms03-026.asp>.
The risk is HIGH. A successful attacker needs only to be able to send an especially crafted packet to port 135 on the target machine. Sites that block port 135 at their incoming firewall are only vulnerable to attack by machines inside of the firewall.

Recommendation: Apply the respective Microsoft patches and block port 135 at your firewall.

Description: There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on specific RPC ports.

Additional Data: <http://www.cert.org/advisories/CA-2003-19.html>

Slide 32

© 2000-2003 by PRESECURE® Consulting GmbH



Alerts – XML / IODEF format

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IODEF-Document>

<IODEF-Document>
  <Incident restriction="eCSIRT.net" purpose="warning">
    <IncidentID>PRE-CERT-0003</IncidentID>
    <IncidentData>
      <Description>eCSIRT.net Test --- A buffer overrun vulnerability exists in the part of the Window
      <Contact role="irt" type="organisation">
        <name>PRE-CERT</name>
        <Email>precert@pre-secure.de</Email>
        <Telephone>+49 40 808077800</Telephone>
        <Fax>+49 40 808077877</Fax>
      </Contact>
      <ReportTime>2003-08-28T10:56+00:00</ReportTime>
      <Expectation category="other: inform constituency">
      </Expectation>
      <Method>
        <Classification origin="vendor">
          <url>http://www.microsoft.com/security/security_bulletins/ms03-026.asp.</url>
        </Classification>
        <Description>The risk is HIGH. A successful attacker needs only to be able to send an especial
      </Method>
      <Assessment>
        <Impact severity="admin" type="high" />
      </Assessment>
      <EventData>
        <Description>Windows: XP NT, Windows 2000, Windows 2003 Server - There is a vulnerability in
      </EventData>
      <AdditionalData>http://www.cert.org/advisories/CA-2003-19.html </AdditionalData>
    </IncidentData>
  </Incident>
</IODEF-Document>
```

Slide 33

© 2000-2003 by PRESECURE® Consulting GmbH



Out-of-the-Internet Alert Function

- The out-of-band function shall be used only
 - If the in-band function isn't available
 - Or outside business hours / during weekends
 - Last resort if no other communication means are available
- Telecommunication application server
 - Isolated LINUX server with GNU Bayonne
 - Caller identification with UID and PIN
- Status
 - Process will be extended based on first test results
 - Operational

Slide 34

© 2000-2003 by PRESECURE® Consulting GmbH



Outlook for the Alert Function

■ Further out-of-the-Internet services:

- Support of SMS
- Automatic FAX distribution to allow transfer of large documents

■ Include teams from other areas:

- Live reports from other time zones
- Early warning during out-of-hours in Europe

Slide 35

© 2000-2003 by PRESECURE® Consulting GmbH



Scientific Coordinator

Dr. Klaus-Peter Kossakowski

WWW: <https://www.pre-secure.de>
 <https://www.pre-secure.com>

Email: kpk@pre-secure.de

Mobil: (+49) 0171 / 5767010

Slide 37

© 2000-2003 by PRESECURE® Consulting GmbH

