CVSS Is a Big Botch

Micha Borrmann

SySS GmbH

October 10th, 2014

SySS THE PENTEST EXPERTS.

HACKTIVITY

Who am I?

Micha Borrmann

- from Germany
- working in information security since 1997

Who am I?

Micha Borrmann

- from Germany
- working in information security since 1997

My Point of View

- I am working at a company which is offering professional penetration tests to help clients to improve their level of IT security
- All examples are based on real professional penetration tests: no company names will be published

Why Scoring

Why Scoring

Management Requirement

Why Scoring

Management Requirement

“If You Can’t Measure It, You Can’t Manage It”

Why Scoring

Management Requirement

“If You Can’t Measure It, You Can’t Manage It”

Client Requirement

Why Scoring

Management Requirement

“If You Can’t Measure It, You Can’t Manage It”

Client Requirement

Please classify our level of IT security with a school grade

School Grades

What does the school grade of 4 in “German” say about the skill level?

School Grades

What does the school grade of 4 in “German” say about the skill level?

Country	Best school grade	Worst school grade
Germany	1	6
Austria	1	5
Switzerland	6	1
Hungary	5	1

School Grades

What does the school grade of 4 in “German” say about the skill level?

Country	Best school grade	Worst school grade
Germany	1	6
Austria	1	5
Switzerland	6	1
Hungary	5	1

Attention

A native speaker of German pupil from Austria or Germany with a school grade of 4 speaks and understands the German language much better than a pupil from Hungary, because even for a good Hungarian pupil German still is a foreign language!

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.
- Our companies website was in the media for being vulnerable to cross-site scripting. This is a very high risk!

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.
- Our companies website was in the media for being vulnerable to cross-site scripting. This is a very high risk!
- We have to introduce 802.1X, to protect our network.

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.
- Our companies website was in the media for being vulnerable to cross-site scripting. This is a very high risk!
- We have to introduce 802.1X, to protect our network.
- The mobile computer of a board member has a virus! This is a topic of major importance!

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.
- Our companies website was in the media for being vulnerable to cross-site scripting. This is a very high risk!
- We have to introduce 802.1X, to protect our network.
- The mobile computer of a board member has a virus! This is a topic of major importance!
- We are lacking some client access licences which is a great risk and will result in a penalty. The missing licences should be purchased soon!

Typical Situations for IT Managers: How to Prioritize?

- The batteries in our business smartphones are empty quickly – our sales representatives can not work efficiently. This is an urgent matter for our business!
- Our DHCP server software is running in a vulnerable version and we have to upgrade our network equipment soon.
- Our companies website was in the media for being vulnerable to cross-site scripting. This is a very high risk!
- We have to introduce 802.1X, to protect our network.
- The mobile computer of a board member has a virus! This is a topic of major importance!
- We are lacking some client access licences which is a great risk and will result in a penalty. The missing licences should be purchased soon!
- All used Android devices are insecure because the same origin policy can be bypassed. This is a very high risk and known as CVE-2014-6041!

Introduction to CVSS

- Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk.

Introduction to CVSS

- Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

Introduction to CVSS

- Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

Introduction to CVSS

- Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.
- With CVSS, anyone can see the individual characteristics used to derive a score.

Introduction to CVSS

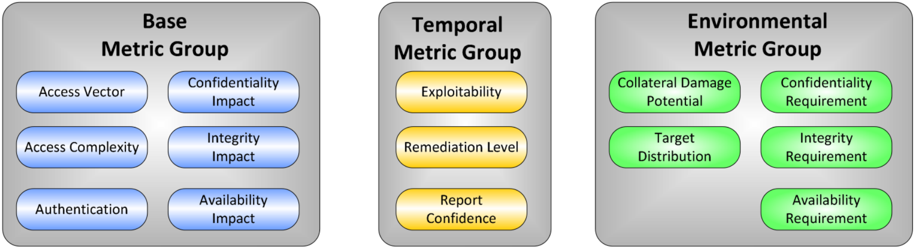
- Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk.
- The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.
- With CVSS, anyone can see the individual characteristics used to derive a score.

Quoted from `http://www.first.org/cvss/cvss-guide`

What is CVSS

CVSS consists of 3 groups:

Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score.



Quoted from `http://www.first.org/cvss/cvss-guide`

Base Metric Group

- The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments.

Base Metric Group

- The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments.
- If desired, the base score can be refined by assigning values to the temporal and environmental metrics. This is useful in order to provide additional context for a vulnerability by more accurately reflecting the risk posed by the vulnerability to a user's environment. **However, this is not required.** Depending on one's purpose, the base score and vector may be sufficient.

Quoted from `http://www.first.org/cvss/cvss-guide`

Base Metric Group

- The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments.
- If desired, the base score can be refined by assigning values to the temporal and environmental metrics. This is useful in order to provide additional context for a vulnerability by more accurately reflecting the risk posed by the vulnerability to a user's environment. **However, this is not required.** Depending on one's purpose, the base score and vector may be sufficient.

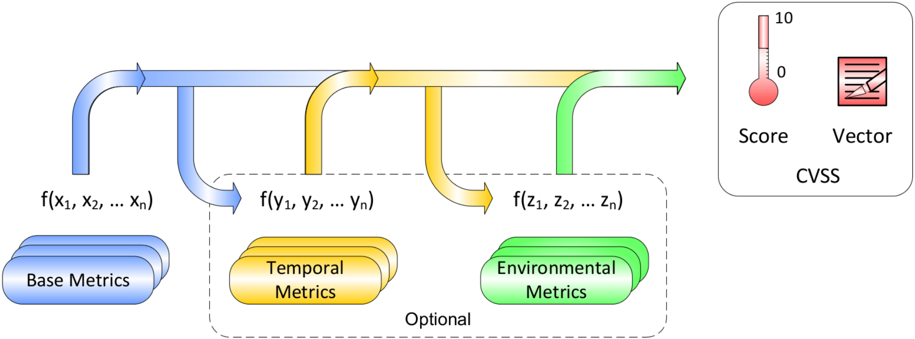
Quoted from `http://www.first.org/cvss/cvss-guide`

Limitation

Only base group in focus of this talk (organizations which are using CVSS often do the same)

How does CVSS work?

When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and a vector is created, as illustrated. The vector facilitates the “open” nature of the framework. **Therefore, the vector should always be displayed with the vulnerability score.**



Quoted from `http://www.first.org/cvss/cvss-guide`

Access Vector (AV)

- This metric reflects how the vulnerability is exploited.
- The more remote an attacker can be to attack a host, the greater the vulnerability score.

Metric Value	Description
Local (L)	A vulnerability exploitable with only local access requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo).
Adjacent Network (A)	A vulnerability exploitable with adjacent network access requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment.
Network (N)	A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable”. An example of a network attack is an RPC buffer overflow.

Quoted from `http://www.first.org/cvss/cvss-guide`

Access Complexity (AC)

- This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will.
- Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment.
- The lower the required complexity, the higher the vulnerability score.
- Possible values are High (H), Medium (M) or Low (L).

Quoted from `http://www.first.org/cvss/cvss-guide`

Authentication (Au)

- This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability.
- The fewer authentication instances that are required, the higher the vulnerability score.
- Possible values are Multiple (M), Single (S) or None (N).

Quoted from `http://www.first.org/cvss/cvss-guide`

Impacts: Confidentiality / Integrity / Availability

Confidentiality Impact (C)

This metric measures the impact on confidentiality of a successfully exploited vulnerability.

Integrity Impact (I)

This metric measures the impact to integrity of a successfully exploited vulnerability.

Availability Impact (A)

This metric measures the impact to availability of a successfully exploited vulnerability. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system.

Possible values for all these metrics

None (N), Partial (P) or Complete (C)

Equation

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20* AccessVector*AccessComplexity*Authentication
f(impact)= 0 if Impact=0, 1.176 otherwise
AccessVector     = case AccessVector of
                        requires local access: 0.395
                        adjacent network accessible: 0.646
                        network accessible: 1.0
AccessComplexity = case AccessComplexity of
                        high: 0.35
                        medium: 0.61
                        low: 0.71
Authentication   = case Authentication of
                        requires multiple instances of authentication: 0.45
                        requires single instance of authentication: 0.56
                        requires no authentication: 0.704
ConfImpact       = case ConfidentialityImpact of
                        none:             0.0
                        partial:          0.275
                        complete:         0.660
IntegImpact      = case IntegrityImpact of
                        none:             0.0
                        partial:          0.275
                        complete:         0.660
AvailImpact      = case AvailabilityImpact of
                        none:             0.0
                        partial:          0.275
                        complete:         0.660
```

Adopters

Who performs the scoring?

The base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors

Quoted from

`http://www.first.org/cvss/cvss-guide`

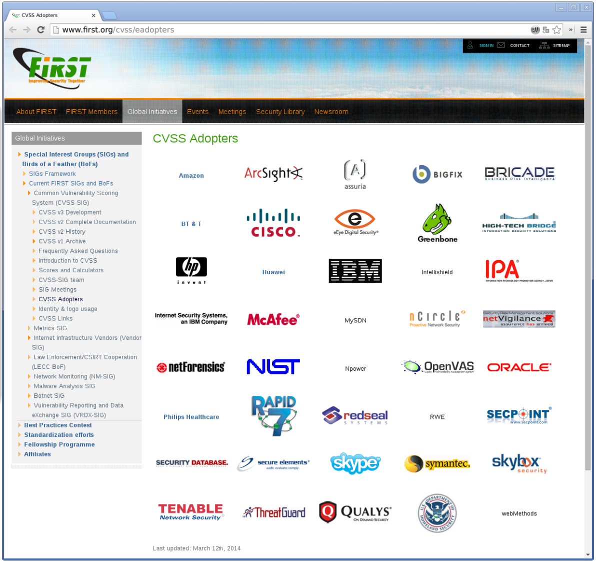
Adopters

Who performs the scoring?

The base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors

Quoted from

`http://www.first.org/cvss/cvss-guide`



CVSS Adopters

Amazon, ArcSight, assuria, BIGFIX, BRICADE Business Risk Intelligence, BT & T, CISCO, eEye Digital Security, Greenbone, HIGH-TECH BRIDGE Information Security Solutions, hp invent, Huawei, IBM, Intellishield, IPA Information-Technology Promotion Agency, Japan, Internet Security Systems, an IBM Company, McAfee, MySDN, nCircle Proactive Network Security, netVigilance, netForensics, NIST, Npower, OpenVAS, ORACLE, Philips Healthcare, RAPID7, redseal systems, RWE, SECPOINT www.secpoint.com, SECURITY DATABASE, secure elements, skype, symantec, skybox security, TENABLE Network Security, ThreatGuard, QUALYS On Demand Security, U.S. Department of Homeland Security, webMethods

Last updated: March 12th, 2014

Short Summary

CVSS

- represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.

Short Summary

- represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- specified from IT security experts

Short Summary

- represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- specified from IT security experts
- calculated with a complex equation

Short Summary

- represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- specified from IT security experts
- calculated with a complex equation
- adopted from many organizations

Useful Examples with Different Scores

MS09-001 – 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code (...) “SMB Buffer Overflow Remote Code Execution Vulnerability.”

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834`

Useful Examples with Different Scores

MS09-001 – 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code (...) “SMB Buffer Overflow Remote Code Execution Vulnerability.”

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834`

MS09-004 – 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

Heap-based buffer overflow in Microsoft SQL Server 2000 SP4, 8.00.2050, 8.00.2039, and earlier; SQL Server 2000 Desktop Engine (MSDE 2000) SP4; SQL Server 2005 SP2 and 9.00.1399.06; SQL Server 2000 Desktop Engine (WMSDE) on Windows Server 2003 SP1 and SP2; and Windows Internal Database (WYukon) SP2 allows remote authenticated users to cause a denial of service (access violation exception) or execute arbitrary code (...)

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5416`

Identical Vulnerabilities Will Result in Identical Score

CVE-2012-6606 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Palo Alto Networks GlobalProtect before 1.1.7, and NetConnect, does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof portal servers and obtain sensitive information via a crafted certificate.

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6606`

Identical Vulnerabilities Will Result in Identical Score

CVE-2012-6606 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Palo Alto Networks GlobalProtect before 1.1.7, and NetConnect, does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof portal servers and obtain sensitive information via a crafted certificate.

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6606`

CVE-2014-2735 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

WinSCP before 5.5.3, when FTP with TLS is used, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate. Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2735`

Identical Vulnerabilities Will Result in Identical Score

CVE-2012-6606 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Palo Alto Networks GlobalProtect before 1.1.7, and NetConnect, does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof portal servers and obtain sensitive information via a crafted certificate.

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6606`

CVE-2014-2735 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

WinSCP before 5.5.3, when FTP with TLS is used, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate. Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2735`

What should be fixed first?

Identical Vulnerabilities Will Result in Identical Score

CVE-2012-6606 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Palo Alto Networks GlobalProtect before 1.1.7, and NetConnect, does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof portal servers and obtain sensitive information via a crafted certificate.

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6606`

CVE-2014-2735 – 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

WinSCP before 5.5.3, when FTP with TLS is used, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate. Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2735`

What should be fixed first?

There the temporal and or environmental score can be used

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority
- a lower score needs a lower priority

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority
- a lower score needs a lower priority
- as a lot of companies and organizations use such a complex equation nobody will recognize a personal mistake for decisions based on CVSS

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority
- a lower score needs a lower priority
- as a lot of companies and organizations use such a complex equation nobody will recognize a personal mistake for decisions based on CVSS
- different tools and a penetration tester will generate comparable results

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority
- a lower score needs a lower priority
- as a lot of companies and organizations use such a complex equation nobody will recognize a personal mistake for decisions based on CVSS
- different tools and a penetration tester will generate comparable results

Everything is ok?

CVSS Summary in Practice

- CVSS: the base score is in use (in most cases only)
- a higher score needs a higher priority
- a lower score needs a lower priority
- as a lot of companies and organizations use such a complex equation nobody will recognize a personal mistake for decisions based on CVSS
- different tools and a penetration tester will generate comparable results

Everything is ok?

Then why you are here?

Example of a Known Limitation

Example of a Known Limitation

Cross-site scripting vulnerability

Example of a Known Limitation

Cross-site scripting vulnerability

The impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact. Cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity.

Quoted from `http://www.first.org/cvss/cvss-guide`

Example of a Known Limitation

Cross-site scripting vulnerability

The impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact. Cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity.

Quoted from `http://www.first.org/cvss/cvss-guide`

Passwords stored in a browser

Example of a Known Limitation

Cross-site scripting vulnerability

The impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact. Cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity.

Quoted from `http://www.first.org/cvss/cvss-guide`

Passwords stored in a browser

can be read out with XSS attack ... no impact on confidentiality?!

XSS and CVSS

- CVSS is focused on target hosts, but IT security issues are related to solutions.

XSS and CVSS

- CVSS is focused on target hosts, but IT security issues are related to solutions.
- For instance: If it is possible to find a XSS vulnerability at `https://signin.ebay.com` to read out stored credentials from a user's browser, do you think there is no impact on confidentiality?

XSS and CVSS

- CVSS is focused on target hosts, but IT security issues are related to solutions.
- For instance: If it is possible to find a XSS vulnerability at `https://signin.ebay.com` to read out stored credentials from a user's browser, do you think there is no impact on confidentiality?
- However, it is true, that there is no impact on confidentiality of the host which provides `https://signin.ebay.com` but nobody asks for such a target host, the solution is in the focus!

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

NIST

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

NIST

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Tenable

6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

NIST

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Tenable

6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

Reason

Different opinion about Access Complexity

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

NIST

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Tenable

6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

Reason

Different opinion about Access Complexity

Base score is constant

Base Score is Constant

CVE-2012-0178 (MS12-033)

Security issue within Windows Partition Manager

NIST

7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Tenable

6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

Reason

Different opinion about Access Complexity

Base score is constant

May be an exception

Identical Vulnerability Results in Identical Score

CVE-2011-0411

Plaintext command injection in multiple implementations of STARTTLS SMTP is not the only protocol with a mid-session switch from plaintext to TLS. Other examples are POP3, IMAP, NNTP and FTP. Implementations of these protocols may be affected by the same flaw as discussed here.

Quoted from `http://www.postfix.org/CVE-2011-0411.html`

Identical Vulnerability Results in Identical Score

CVE-2011-0411

Plaintext command injection in multiple implementations of STARTTLS SMTP is not the only protocol with a mid-session switch from plaintext to TLS. Other examples are POP3, IMAP, NNTP and FTP. Implementations of these protocols may be affected by the same flaw as discussed here.

Quoted from `http://www.postfix.org/CVE-2011-0411.html`

FTP Service AUTH TLS Plaintext Command Injection

The STARTTLS implementation (...) a similar issue to CVE-2011-0411.

Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1575`

Plaintext Command Injections within STARTTLS

SMTP

Plaintext Command Injections within STARTTLS

Tenable / Redhat (CVE-2011-0411)

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

SMTP

Plaintext Command Injections within STARTTLS

SMTP

Tenable / Redhat (CVE-2011-0411)

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

NIST (CVE-2011-0411)

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Plaintext Command Injections within STARTTLS

SMTP

Tenable / Redhat (CVE-2011-0411)

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

NIST (CVE-2011-0411)

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

FTP

Plaintext Command Injections within STARTTLS

SMTP

Tenable / Redhat (CVE-2011-0411)

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

NIST (CVE-2011-0411)

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

FTP

Tenable / NIST (CVE-2011-1575)

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Redhat (CVE-2011-1575)

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

Firewall Filter Bypass Vulnerability

Similar vulnerabilities: CVE-2003-1491 & CVE-2004-1473

Some firewalls can be bypassed with UDP source port 53.

Firewall Filter Bypass Vulnerability

Similar vulnerabilities: CVE-2003-1491 & CVE-2004-1473

Some firewalls can be bypassed with UDP source port 53.

Tenable (both) / NIST (CVE-2003-1491)

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Firewall Filter Bypass Vulnerability

Similar vulnerabilities: CVE-2003-1491 & CVE-2004-1473

Some firewalls can be bypassed with UDP source port 53.

Tenable (both) / NIST (CVE-2003-1491)

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

NIST (CVE-2004-1473)

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

SSL Version 2 Support for a TLS Protected Service

SSL Version 2 Support for a TLS Protected Service

Tenable

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

SSL Version 2 Support for a TLS Protected Service

Tenable

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

SSL Version 2 Support for a TLS Protected Service

Tenable

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Rapid7

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

SSL Version 2 Support for a TLS Protected Service

Tenable

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Rapid7

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

PCI (Payment Card Industry) Data Security Standard

Support of SSLv2 will result in not getting the certificate

More Examples with Bad Crypto

CVE-2004-2761

This vulnerability described MD5-based signatures in TLS/SSL Server X.509 Certificate

More Examples with Bad Crypto

CVE-2004-2761

This vulnerability described MD5-based signatures in TLS/SSL Server X.509 Certificate

Rapid7 / NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

More Examples with Bad Crypto

CVE-2004-2761

This vulnerability described MD5-based signatures in TLS/SSL Server X.509 Certificate

Rapid7 / NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

More Examples with Bad Crypto

CVE-2004-2761

This vulnerability described MD5-based signatures in TLS/SSL Server X.509 Certificate

Rapid7 / NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Tenable

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

More Examples with Bad Crypto II

CVE-2013-2566

Usage of RC4

More Examples with Bad Crypto II

CVE-2013-2566

Usage of RC4

NIST / Tenable

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

More Examples with Bad Crypto II

CVE-2013-2566

Usage of RC4

NIST / Tenable

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Redhat

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

More Examples with Bad Crypto II

CVE-2013-2566

Usage of RC4

CVE-2012-4929

Vulnerability called CRIME

NIST / Tenable

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Redhat

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

More Examples with Bad Crypto II

CVE-2013-2566

Usage of RC4

NIST / Tenable

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Redhat

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVE-2012-4929

Vulnerability called CRIME

NIST

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

More Examples with Bad Crypto II

CVE-2013-2566	CVE-2012-4929
Usage of RC4	Vulnerability called CRIME
NIST / Tenable	**NIST**
2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)
Redhat	**Redhat / Tenable**
4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

Weak RSA key (less than 2048 bit length)

Tenable

No CVSS value!

`http://www.tenable.com/plugins/index.php?view=single&id=69551`

Weak RSA key (less than 2048 bit length)

Tenable

No CVSS value!

`http://www.tenable.com/plugins/index.php?view=single&id=69551`

Rapid7

3.2 (AV:A/AC:H/Au:N/C:P/I:P/A:N)

CVE-2014-0160

CVE-2014-0160

CVE-2014-0160

NIST, Redhat, Rapid7

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE-2014-0160

NIST, Redhat, Rapid7

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Tenable

9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

CVE-2014-0160

NIST, Redhat, Rapid7

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Tenable

9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

Bruce Schneier

“Catastrophic” is the right word. On the scale of 1 to 10, this is an 11.

https://www.schneier.com/blog/archives/2014/04/heartbleed.html

CVE-2014-6271

CVE-2014-6271

CVE-2014-6271

Redhat

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE-2014-6271

Redhat

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

NIST

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

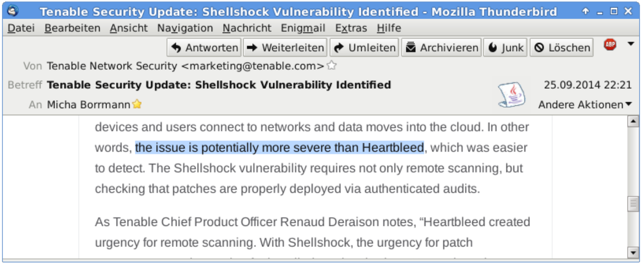
CVE-2014-6271

Redhat

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

NIST

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)



Tenable Security Update: Shellshock Vulnerability Identified - Mozilla Thunderbird
Datei Bearbeiten Ansicht Navigation Nachricht Enigmail Extras Hilfe
Antworten
Weiterleiten
Umleiten
Archivieren
Junk
Löschen
Andere Aktionen

Von Tenable Network Security <marketing@tenable.com>

Betreff **Tenable Security Update: Shellshock Vulnerability Identified** 25.09.2014 22:21

An Micha Borrmann

devices and users connect to networks and data moves into the cloud. In other words, the issue is potentially more severe than Heartbleed, which was easier to detect. The Shellshock vulnerability requires not only remote scanning, but checking that patches are properly deployed via authenticated audits.

As Tenable Chief Product Officer Renaud Deraison notes, "Heartbleed created urgency for remote scanning. With Shellshock, the urgency for patch

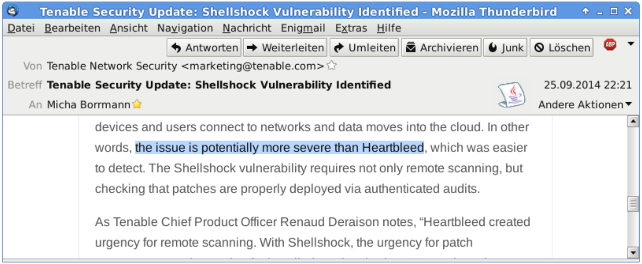
CVE-2014-6271

Redhat

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

NIST

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)


Tenable Security Update: Shellshock Vulnerability Identified - Mozilla Thunderbird
Datei Bearbeiten Ansicht Navigation Nachricht Enigmail Extras Hilfe
Antworten
Weiterleiten
Umleiten
Archivieren
Junk
Löschen
Andere Aktionen

Von Tenable Network Security <marketing@tenable.com>

Betreff **Tenable Security Update: Shellshock Vulnerability Identified** 25.09.2014 22:21

An Micha Borrmann

devices and users connect to networks and data moves into the cloud. In other words, the issue is potentially more severe than Heartbleed, which was easier to detect. The Shellshock vulnerability requires not only remote scanning, but checking that patches are properly deployed via authenticated audits.

As Tenable Chief Product Officer Renaud Deraison notes, "Heartbleed created urgency for remote scanning. With Shellshock, the urgency for patch

Tenable

"(...) the issue is potentially more severe than Heartbleed (...)"

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Tenable (now)

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Tenable (April 2012 until ?)

2.6 (AV:N/AC:H/Au:N/C:N/I:N/A:P)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

`https://discussions.nessus.org/thread/4608`

Tenable (now)

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Base Score (...) Constant over Time

CVE-2011-1473 (SSL Renegotiation)

Disputed OpenSSL (...) does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection (...) Quoted from `http://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473`

NIST

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

Redhat

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Tenable (now)

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Tenable (April 2012 until ?)

2.6 (AV:N/AC:H/Au:N/C:N/I:N/A:P)

`https://discussions.nessus.org/thread/4608`

Tenable (May 2011 until ?)

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

`https://discussions.nessus.org/message/10629`

10. Crypto Bug

10. Crypto Bug

CVE-2014-0224

OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

10. Crypto Bug

CVE-2014-0224

OpenSSL ’ChangeCipherSpec’ MiTM Potential Vulnerability

NIST, Rapid7

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

10. Crypto Bug

CVE-2014-0224

OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

NIST, Rapid7

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Redhat, Tenable at June 6, 2014

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

http://www.tenable.com/blog/detect-the-latest-openssl-vulnerabilities-using-active-and-passive-scanning

10. Crypto Bug

CVE-2014-0224

OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

NIST, Rapid7

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Redhat, Tenable at June 6, 2014

5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

http://www.tenable.com/blog/detect-the-latest-openssl-vulnerabilities-using-active-and-passive-scanning

Tenable at least since June 18, 2014

9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS: First Conclusion

CVSS: First Conclusion

- CVSS base score is not constant over time

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties
- Use only one source for your CVSS scores for a specific date

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties
- Use only one source for your CVSS scores for a specific date

Example: What has to be fixed firstly?

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties
- Use only one source for your CVSS scores for a specific date

Example: What has to be fixed firstly?

Use only NIST

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties
- Use only one source for your CVSS scores for a specific date

Example: What has to be fixed firstly?

Use only NIST

- CVE-2011-0411: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
- CVE-2014-0224: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
- CVE-2014-2735: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
- CVE-2014-0160: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS: First Conclusion

- CVSS base score is not constant over time
- CVSS base score will be calculated differently by different parties
- Use only one source for your CVSS scores for a specific date

Example: What has to be fixed firstly?

Use only NIST

CVE-2011-0411: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	STARTTLS
CVE-2014-0224: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	OpenSSL CCS
CVE-2014-2735: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	WinSCP
CVE-2014-0160: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	Heartbleed

Improve IT Security with Decreasing CVSS Score

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

- CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
- CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
- CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
- CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution:

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

FTP Supports Clear Text Authentication: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

FTP Supports Clear Text Authentication: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Conclusion

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

FTP Supports Clear Text Authentication: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Conclusion

- knowledge of vulnerabilities is necessary for prioritization

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

FTP Supports Clear Text Authentication: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Conclusion

- knowledge of vulnerabilities is necessary for prioritization
- the score does not help for prioritization to improve the IT security

Improve IT Security with Decreasing CVSS Score

Vulnerable FTP/TLS service (Tenable)

CVE-2011-1473: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	Renegotiation
CVE-2011-1575: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)	STARTTLS
CVE-2014-0224: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	OpenSSL CCS
CVE-2013-2566: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)	RC4

Solution: Disable encryption!

FTP Supports Clear Text Authentication: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Conclusion

- knowledge of vulnerabilities is necessary for prioritization
- the score does not help for prioritization to improve the IT security
- if kowledge is available, nobody needs a score

Summary CVSS

CVSS

- no common score for identical vulnerabilities

Summary CVSS

CVSS

- no common score for identical vulnerabilities
- no help for prioritization deploying fixes against vulnerabilities

Summary CVSS

CVSS

- no common score for identical vulnerabilities
- no help for prioritization deploying fixes against vulnerabilities
- focussing on hosts will not cover real situations of IT security (think about the example with XSS)

Do not use CVSS!

Do not use CVSS!

- managers for prioritization for deploy fixes

Do not use CVSS!

- managers for prioritization for deploy fixes
- researcher for promoting a found weakness

Do not use CVSS!

- managers for prioritization for deploy fixes
- researcher for promoting a found weakness
- security bulletin providers for announcing advisories because the score is not helpful

And Now?

And Now?

- CVSS v3 (Preview June 2014)

And Now?

- CVSS v3 (Preview June 2014) No

And Now?

- CVSS v3 (Preview June 2014)
- Common Weakness Scoring System (CWSS^{TM})

No

And Now?

- CVSS v3 (Preview June 2014) No
- Common Weakness Scoring System (CWSS$^{\text{TM}}$) No

And Now?

• CVSS v3 (Preview June 2014)	No
• Common Weakness Scoring System (CWSS^{TM})	No
• Develop a new scoring system	

And Now?

- CVSS v3 (Preview June 2014) No
- Common Weakness Scoring System (CWSS$^{\text{TM}}$) No
- Develop a new scoring system No

And Now?

CVSS v3 (Preview June 2014)	No
Common Weakness Scoring System (CWSS^{TM})	No
Develop a new scoring system	No
Scoring is a technology	

And Now?

- CVSS v3 (Preview June 2014) No
- Common Weakness Scoring System (CWSS^{TM}) No
- Develop a new scoring system No
- Scoring is a technology

https://www.schneier.com/book-sandl-pref.html

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Information for the World's Business Leaders

Article on Forbes website (February 10, 2014)

Information for the World's Business Leaders

Article on Forbes website (February 10, 2014)

'If You Can't Measure It, You Can't Manage It':

Information for the World’s Business Leaders

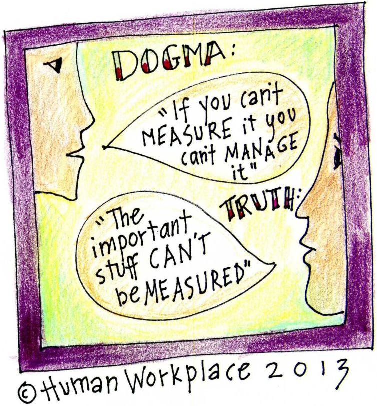
Article on Forbes website (February 10, 2014)

’If You Can’t Measure It, You Can’t Manage It’: Not True

Information for the World’s Business Leaders

Article on Forbes website (February 10, 2014)

’If You Can’t Measure It, You Can’t Manage It’: Not True


DOGMA:
"If you can't MEASURE it you can't MANAGE it"
TRUTH:
"The important stuff CAN'T be MEASURED"
©Human Workplace 2013

A typical ridiculous, unquestioned business adage is “If you can’t measure it, you can’t manage it.” That’s BS on the face of it, because the vast majority of important things we manage at work aren’t measurable, from the quality of our new hires to the confidence we instill in a fledgling manager.

Quoted from `http://onforb.es/1fXmIkJ`

Information for the World's Business Leaders (II)

- *We love to measure things, because it makes us feel as though we're really doing something.*

Information for the World's Business Leaders (II)

- *We love to measure things, because it makes us feel as though we're really doing something.*
- *Measurement is our drug in the business world, because we believe that by measuring everything and sending the good news upstairs to the C-suite we can ward off the bogeyman of business, namely Getting On the Boss's Bad Side.*

Information for the World’s Business Leaders (II)

- *We love to measure things, because it makes us feel as though we’re really doing something.*
- *Measurement is our drug in the business world, because we believe that by measuring everything and sending the good news upstairs to the C-suite we can ward off the bogeyman of business, namely Getting On the Boss’s Bad Side.*
- *Measurement (...) is an inherently fear-based process, because the reason we measure everything in business is to prove to someone who’s not in the room that we did what they told us to do.*

Information for the World's Business Leaders (II)

- *We love to measure things, because it makes us feel as though we're really doing something.*
- *Measurement is our drug in the business world, because we believe that by measuring everything and sending the good news upstairs to the C-suite we can ward off the bogeyman of business, namely Getting On the Boss's Bad Side.*
- *Measurement (...) is an inherently fear-based process, because the reason we measure everything in business is to prove to someone who's not in the room that we did what they told us to do.*
- *Measurement is our opiate of choice in the business world precisely because it temporarily allays fear all the way up the ladder. Look boss, there's the number, right there on the chart – I hit the mark, so don't blame me!*

Quoted from `http://www.forbes.com/sites/lizryan/2014/02/10/if-you-cant-measure-it-you-cant-manage-it-is-bs/`

Final: Short Summary

Conclusion from Forbes article

If data IT security is important stuff, than it can not be measured!

Final: Short Summary

Conclusion from Forbes article

If data IT security is important stuff, than it can not be measured!

Easy to remember slogan

Final: Short Summary

Conclusion from Forbes article

If data IT security is important stuff, than it can not be measured!

Easy to remember slogan

use it
and you will lose it

Final: Short Summary

Conclusion from Forbes article

If data IT security is important stuff, than it can not be measured!

Easy to remember slogan

use it	(scoring systems for IT security like CVSS)
and you will lose it	(IT security)

Thank You for Your Attention

E-Mail

`micha.borrmann@syss.de`

PGP fingerprint:

`6897 7B33 B359 B8BA 0884 969F FC67 EBA9 1B51 128A`